MAKING SPACE

Clearing the Way for Hybrid Architecture

March 2026

POTOMAC INSTITUTE
FOR POLICY STUDIES

Making Space: Clearing the Way for Hybrid Architecture

ABOUT THE POTOMAC INSTITUTE FOR POLICY STUDIES

The Potomac Institute for Policy Studies is an independent, nonpartisan, 501(c)(3), non-profit science and technology policy research institute. The Institute identifies and leads discussion on key science and technology issues facing our society. From these discussions and forums, we develop meaningful policy recommendations and ensure their implementation at the intersection of business and government.

FURTHER INFORMATION AND PERMISSIONS MAY BE REQUESTED FROM:

Potomac Institute for Policy Studies

Email: info@potomacinstitute.org

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

EXECUTIVE SUMMARY

Space is now a vibrant international and commercial theater of operations for the US military, industry, intelligence, allies, and adversaries. As physical and economic wars threaten the globe, protecting national interests will not be achievable by relying solely on traditional, military-owned space systems. **To secure our nation's interests in space, enhance its utility to US assets on the ground, and protect the country from orbital threats, the United States Space Force (USSF) must fully leverage and integrate Intelligence Community (IC), civil, commercial, and international capabilities into a hybrid architecture.**

As the pace of technological change in space increases, an effective hybrid architecture will provide the speed, capacity, interoperability, and resilience to deter and, if necessary, defeat adversaries like China. **In fact, this winning approach is the only one that is effective, feasible, and affordable.**

The USSF is actively pursuing a hybrid architecture, but the effort is not as fully coordinated and integrated as required. Legal and policy barriers, both real and perceived, are slowing adoption. This leaves the United States in a riskier strategic position relative to adversaries like China, whose hybrid architecture, uninhibited by such barriers, is advancing rapidly.

This study focused on identifying, understanding, and mitigating legal and policy barriers to adopting a hybrid architecture. The findings and recommendations provide a foundation for the USSF, and the United States more broadly, to accelerate achievement of an effective hybrid architecture. **The earlier the United States identifies and mitigates the risks and barriers associated with the pivot to a hybrid architecture, the faster, smoother, and more effective the transition will be.**

Finding 1: Dozens of laws, policies, and events pose potentially critical hurdles to a hybrid architecture; all can be overcome.

Of 389 distinct laws, policies, and precedent-setting geopolitical events related to a hybrid architecture, dozens pose potentially critical hurdles. None are insurmountable. Outdated statutes and policies—some dating as far back as the 1950 Defense Production Act—need to be reviewed and, where necessary, revised.

Recommendation 1: Remove critical legal and policy barriers by chartering a Hybrid Architecture Task Force to lead hybrid architecture baselining, barrier fact finding, and needed policy and legislative changes.

The USSF should charter a Hybrid Architecture Task Force, potentially driven by the Chief of Space Operations' Strategic Initiatives Group. This group should baseline the hybrid architecture and associated barriers and aggressively advocate for the policy changes needed to remove critical obstacles. The Task Force's priority mission[1] should focus on near-term activity.

[1] For example, Ground Moving Target Indicator/Air Moving Target Indicator (GMTI/AMTI) for kill chains, or space elements of Next Generation Missile Defense.

Finding 2: USSF delays in fully adopting modern data-centric solutions could paralyze combat operations.

Antiquated, risk-averse mission data and cybersecurity postures hinder operations and slow adoption of modern tools to assure data fidelity. Confusion and misinformation permeate both acquisition and operations regarding the extent to which IC, civil, commercial, and international elements of the hybrid architecture can be "trusted" or used in combat operations. Confusion and resistance arise, in part, from insufficient exposure to, and hesitant embrace of, modern cyber and data-centric tools such as artificial intelligence and machine learning (AI/ML) commonly used in commercial systems.

Recommendation 2: Mitigate data fidelity risks by embracing mission command, zero trust, and modern data and cyber tools.

Empower, task, and resource commanders to accelerate adoption of a hybrid architecture by acquiring and fully using IC, civil, commercial, and international data, starting today. Adopt a zero trust framework[2] with modern data management, cybersecurity, and processing tools and incorporate lessons from US Transportation Command (USTRANSCOM) and at-scale commercial implementations. Consider starting with Ground Moving Target Indicator/Air Moving Target Indicator (GMTI/AMTI) and Tactical Surveillance, Reconnaissance, and Tracking (TacSRT) mission areas to support kill chain operations at scale, in the presence of peer threats, and on rapid planning timelines.

Accelerating a full, smooth, and deliberate pivot to a hybrid space architecture is necessary and achievable, but not trivial. Risks and barriers to accelerating a hybrid architecture exist. They must be illuminated and should be carefully navigated. Deliberate effort will be required to revise antiquated policies and shift cultural predispositions. **Nevertheless, delay or hesitation is the greater risk.**

The DoD and USSF already have most of the legal and policy tools required to begin implementing the recommendations and advocating for requisite legislative changes. As they begin implementing hybrid architecture, the deterrence and warfighting benefits will quickly accrue and outweigh any additional risks and barriers that emerge.

A unifying thread throughout this report echoes the Roman writer Vegetius: "*Si vis pacem, para bellum*" (If you want peace, prepare for war). The USSF must prepare the hybrid architecture for war.

The DoD and USSF must prudently and deliberately double down on hybrid architecture, with speed but also through coordination and integration across missions and potential partners. This ensures that potential barriers are proactively resolved, and the expected mission benefit of peace through strength is realized across the enterprise and full spectrum of conflict.

[2] For a more in-depth exploration of this issue, see "Potomac Institute for Policy Studies. (2024). *Never Trust, Always Verify: Improving Cybersecurity in Hybrid Architectures for Space*. https://www.potomacinstitute.org/papers/never-trust-always-verify-improving-cybersecurity-in-hybrid-architectures-for-space.

INTRODUCTION

The twenty-first century has already seen remarkable change and advancement in the space domain, including reusable launch systems, commercial human spaceflight, proliferated low Earth orbit (LEO) constellations, and more. US and allied military forces rely on space assets and capabilities more every day. Commercial systems have greatly expanded the flow of private capital into space and widened the availability of space.

At the same time, adversary use of space and potential counterspace capabilities has grown significantly, leading to policy and organizational changes within the US government (USG). These changes include standing up the US Space Force and re-establishing US Space Command. Many allied nations have made their own organizational and policy shifts toward incorporating space as a warfighting domain. Amid this landscape of multi-faceted change is an opportunity to harness new synergies.

Next-generation space warfighting will be fought by a hybrid force from the National Security Space Enterprise (which includes systems from the DoD, IC, and civil organizations), integrated commercial space capabilities, as well as allied and foreign partnerships. **The success of that warfighting effort, however, rests upon a knot of overlapping, and sometimes counteracting, laws and policies that accumulated across multiple generations.** Some are beyond DoD and USSF authority to modify on their own. However, there are significant areas where adjustments in USSF policy, planning, and prioritization can accelerate an effective hybrid architecture and secure American superiority in space.

Hybrid Architecture Defined*

Hybrid architecture is the concept of seamless integration between commercial- and government-owned systems, regardless of their country of origin. Just as space is the ultimate global commons, the goal of a hybrid architecture is the "borderless" operation of government-owned and commercial space systems, to the benefit of all, in a fully participative manner.[3]

A hybrid architecture is composed of three major components: **a USG component with elements from the DoD, IC, and civil agencies; an international component** with elements from allies and foreign partners; and a **commercial component** with both domestic and foreign capabilities and services.

Hybrid architectures are network integrated and interoperable. Hybrid architectures must be able to rapidly connect and exchange data among satellite systems and services. Moreover, they must do so whether the systems are large or small, government or commercial, US or allied, and across various orbits.

* Additional key definitions may be found in Appendix C: Definitions.

[3] SmallSat Alliance. (n.d.). *Hybrid Space Architecture Statement of Principles*. SmallSat Alliance. https://smallsatalliance.org/wp-content/uploads/2020/09/Hybrid-Architecture-Statement-of-Principles-v21.pdf.

STATEMENT OF THE PROBLEM

The United States requires specific space capabilities to support an ever-increasing cadence of commercial, civilian, and national security operations. Resilience, deterrence, and protection against identified threats cannot be achieved with US sovereign-only assets. To gain and maintain advantage over rapidly accelerating adversarial capabilities, the USSF is leveraging commercially available innovations and key capabilities of foreign partners and allies. Only through a partnership between commercial and governmental capabilities can we continually improve the reliability, breadth, and depth of space operations.

The need for and adoption of a hybrid architecture are not theoretical; they reflect the commitment of DoD and USSF leadership to accelerate hybrid architecture application for DoD missions. **Although the USSF is pursuing a hybrid architecture through several initiatives, the overall effort is not as comprehensive, fully coordinated, synchronized, and integrated as it needs to be to keep pace with threats. Legal and policy barriers, both real and perceived, are slowing adoption.** This leaves the United States in a position of greater strategic risk in its ability to deter and defeat adversaries like China, whose hybrid architecture, uninhibited by such barriers, is advancing rapidly.

This study identified and recommended ways to mitigate legal and policy risks and barriers to accelerating the deployment of an operationally effective hybrid architecture.

This report presents a novel analytic framework for characterizing those risks and barriers, then demonstrates the power of this framework using the following specially selected subset of USSF missions and Design Reference Mission (DRM) enablers:

- Satellite Communications (SATCOM)
- Space Control
- Tactical Surveillance, Reconnaissance, and Tracking (TacSRT)

The recommendations included provide a means for the USSF to remove these legal and policy barriers to hasten achievement of a fully integrated and effective hybrid architecture.

A **Design Reference Mission (DRM)** is a use case scenario to guide the design and evaluation of systems or architectures.

BACKGROUND: HISTORICAL SPACE POLICIES AND LAWS

Early in the space age, US policymakers quickly appreciated the importance and distinctiveness of space for scientific, technical, military, and intelligence purposes. Over the next several decades, key policy documents, assessments, and treaties were crafted that shape American and global space operations. Many of these documents still impact operations today (see Figure 1, Timeline of Key Space Policy and Law).

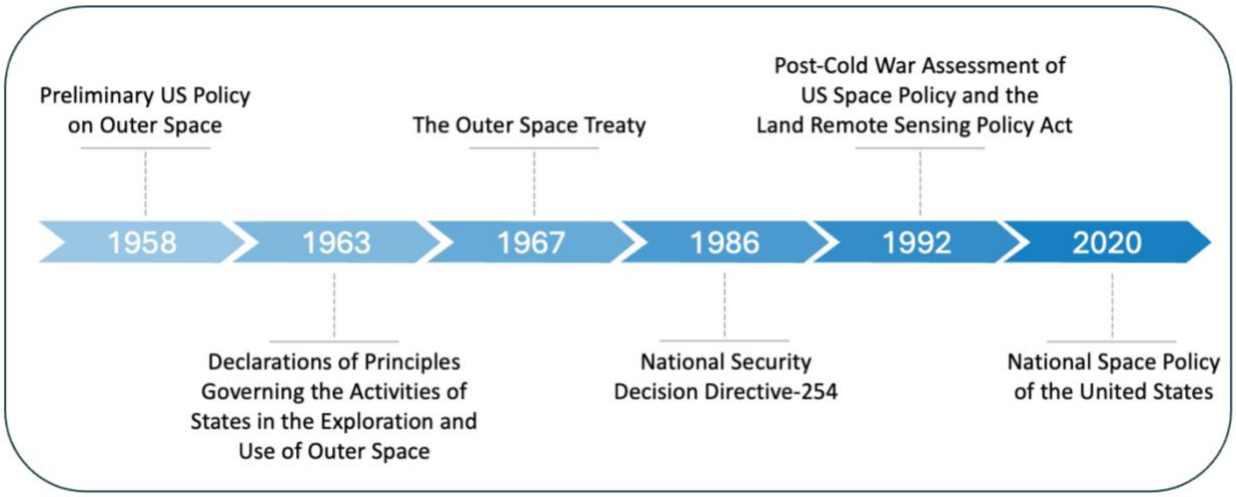

Figure 1. Timeline of Key Space Policy and Law

Several of these policies and laws unveiled policy and legal challenges still facing the United States today. The 1992 Post-Cold War Assessment of US Space Policy, for example, remains salient three decades later (see Figure 2). This continued salience speaks to those recommendations' inherent importance and, potentially, their enduring applicability. A deeper exploration of hybrid architecture legal considerations will be set out in a forthcoming Potomac Institute publication.

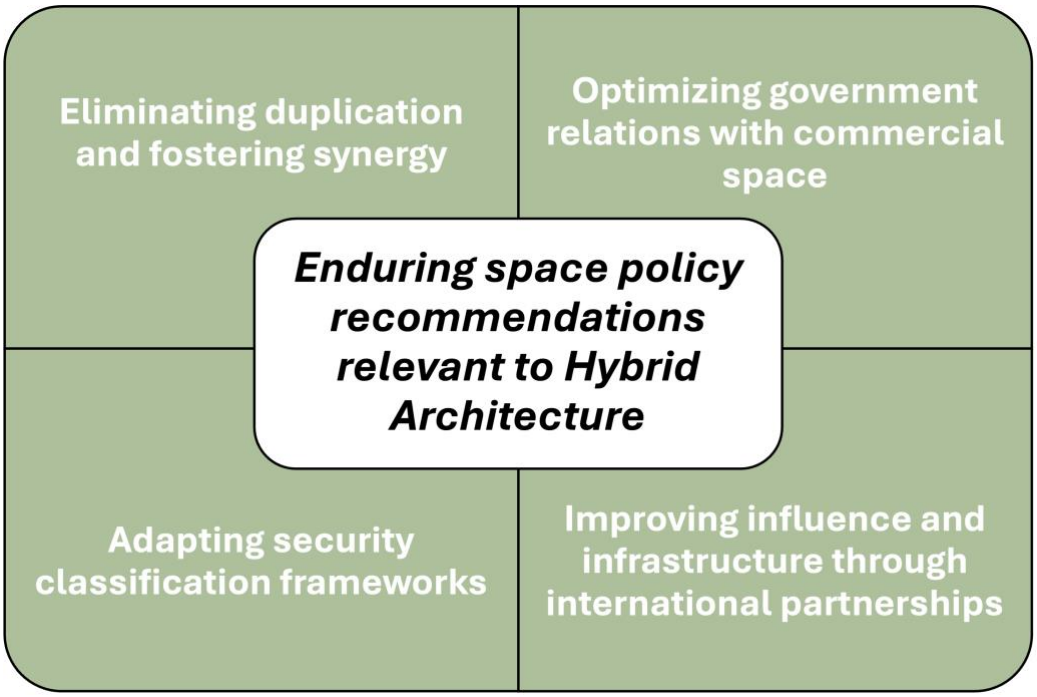

Figure 2. Enduring Space Policy Recommendations (1992-2020)

Since 2020, work by the Defense Innovation Unit and Space Development Agency has accelerated the growth of a hybrid architecture, with more work in development. As progress on these principles continues, it becomes even more critical to identify and remove barriers to hybrid architecture, and to strengthen and codify enablers where necessary. Today, the USSF proposes to unite a host of different space activities with new potential barriers into an expanded hybrid architecture. These activities and capabilities emerged and matured in different ways, for different purposes, and are currently conducted and regulated by different organizations. Each of those organizations also has its own structure and culture, reflecting the political, operational, strategic, and economic interests that drive it.

Yet the diversity of components and cultures inside a hybrid architecture can be leveraged as a strength, not only as a literal marketplace of ideas but also for USSF coordination. Through hybrid architecture, the USSF as an enterprise will be able to exert influence over some aspects of the organization and culture of its disparate USG, commercial, and international components to assemble the best of each element. However, the study anticipated navigating various space enterprise governance processes as they exist.

HYBRID ARCHITECTURE VALUE PROPOSITION

Ensuring American space superiority is a continuous priority that helps secure the nation's vital economic and security interests. Space superiority is not fixed; it must always evolve to match the current moment and threat. Adversaries' abilities to threaten US and friendly forces in and from the space domain jeopardize multi-domain operations. Today, the commercial sector plays an increasingly vital innovation and infrastructure role in the space domain, including support for government operations.

Without an effective hybrid architecture, access to space is compromised, and the ability to operate freely in the domain is at risk. An effective hybrid architecture also provides numerous operational, tactical, and strategic benefits, including:

Resiliency:

1. Providing the capacity, redundancy, and diversity required to deter and, when necessary, defeat adversaries and complicate adversary targeting
2. Creating strength in numbers, distributing risk, and mitigating the acute vulnerability associated with small numbers of high-value assets

Technology Advantage:

1. Operating and innovating faster with rapid insertion of new technologies such as AI/ML as they mature
2. Improving interoperability among US and allied military services and civil and commercial space capability providers
3. Achieving greater space superiority to better operate in all warfighting domains

Decision Advantage:

1. Enhancing situational awareness, informational advantage, and improving operational decision-making to aid commanders directing forces
2. Offering alternate pathways to achieve mission objectives in the presence of advanced non-kinetic operations, such as electromagnetic and cyber warfare

3. Providing new information advantages beyond warfighting functions through rapid collection and dissemination of science, commerce, and security information

SCOPE OF STUDY

The primary goal of this study was to identify policy and legal risks to hybrid architecture for space domain warfighting and propose recommendations to overcome these barriers. The research team compiled and collected an array of data to conduct a three-stage research methodology:[4]

1. Developing an analytic framework relying on a historiography of space law and policy, as well as qualitative comparative analysis of USG programs of record with characteristics similar to hybrid architecture
2. Creating a multi-method risk assessment using quantitative document analysis and qualitative interview analysis
    a. Developing an exploratory case study of the Commercial Augmentation Space Reserve program, which will be detailed in a forthcoming Potomac Institute publication
3. Externally validating the analytic findings through reviews with a dedicated Red Team and a Technical Advisory Team

This report advances a novel analytic framework for characterizing policy and legal risks to accelerate the deployment of an effective hybrid architecture. To highlight how this framework functions, the team examined USSF-selected DRM enablers: SATCOM, Space Control, and TacSRT. These DRMs cover a wide spectrum of use and ownership, from predominantly commercial to predominantly USG-owned and USG-operated. This range is necessary to provide the appropriate breadth and depth for analysis. They also demonstrate potential challenges to a rapidly useful and robust operational hybrid architecture.

It should be noted that this report does not perform a technical analysis of current or proposed hybrid architecture. It also does not address or assess the current resource allocation or staffing disconnects of the status quo hybrid architecture as it exists today.

Rather, guided by the Statement of the Problem above, the analysis explicitly focuses on legal and policy risks to hybrid architecture through the lens of operational barriers, and others. It does so by specifically considering DRM enablers and sample missions that highlight policy and legal risk in selected areas. After completing a risk analysis, the team produced key findings and recommendations needed to accelerate hybrid architecture employment for operational advantage.

[4] A full discussion of the research methodology is located in Appendix B: Research Methodology.

KEY ASSUMPTIONS

To fulfill the requirements of the study, certain assumptions had to be made, which are listed below.

1. Hybrid architectures for space already exist and are in use today.
2. The USSF and DoD have committed to maturing and operating a hybrid architecture in space and to making it effective for future space warfighting.
3. Successful hybrid architectures must be designed for technical interoperability; ad-hoc participation is not a viable approach.
4. Commercial space missions can be integrated into an interoperable hybrid architecture consistent with Law of Armed Conflict and international outer space laws/treaties.
5. Use of commercial capabilities in a space hybrid architecture is analogous to the use of commercial capabilities within the air, land, and maritime domains.
6. Timelines for recommendations should focus on mid-term (18 months–5 years) and long term (5+ years). Recommendations should make hybrid architecture faster, better, and cheaper.
7. USSF leadership remains committed to the objectives and ideals in the following documents: *Space Warfighting: A Framework for Planners* (March 2025), *USSF Commercial Space Strategy* (April 2024), and *USSF International Partnership Strategy* (June 2025).
8. The DoD remains committed to the Acquisition Transformation Strategy of 2025 emphasizing speed, agility, and empowerment for obtaining and integrating warfighting capabilities.
9. The term "international" includes both formally recognized allies and foreign partners of varying levels of capability and relationships with the United States.
10. Intellectual property issues (broadly framed to include patent, copyright, trade secrets, export control, and foreign ownership/control issues) will remain a challenge for a hybrid architecture. These have mature legal and regulatory frameworks with many stakeholders across the USG.
11. Commercial solution providers will continue to protect intellectual property and capital and look for ways to be protected by and from the government.
12. Classification issues will be an enduring condition, regardless of solutions. Legal and policy authorities to classify and declassify space-related information exist, but the complexity of coordination and review processes among stakeholders with varying risk tolerance is continuous.

GUIDING REFERENCES

To guide the analysis, the research team examined a database of 389 distinct laws, policies, and major geopolitical events related to hybrid architecture spanning 1950 through 2025. From this database, several "guide star" documents were selected, representing current leadership commitments and priorities related to the implementation of a hybrid architecture for USSF operations. As noted above, the team assumed that these priorities and efforts will continue through the implementation and maturing of hybrid architecture. The selected documents are listed below and grouped by command structure.

Executive Office of the President of the United States

- *National Security Strategy* (November 2025)
- White House Executive Order—*Ensuring American Space Superiority* (December 18, 2025)

Department of Defense (DoD)

- *DoD Commercial Space Integration Strategy* (2024)
- *Acquisition Transformation Strategy* (2025)
- Sec DoD Memo: *Transforming the Defense Acquisition System into the Warfighting Acquisition System (WAS)* (November 7, 2025)

United States Space Command (USSPACECOM)

- *USSPACECOM Commercial Integration Strategy* (2024)

United States Space Force (USSF)

- *USSF Commercial Space Strategy: Accelerating the Purposeful Pursuit of Hybrid Space Architectures* (2024)
- *USSF International Partnership Strategy: Strength Through Partnership* (2025)
- *Space Warfighting: A Framework for Planners* (2025)

ANALYTIC FRAMEWORK

Hybrid architecture offers significant benefits but, as the USSF has acknowledged, it also contributes risk and uncertainty.[5] Understanding, managing, and mitigating those risk factors is critical to the success of hybrid architecture programs. Beyond technical considerations of constructing such an architecture, there are significant challenges to managing the legal and policy implications to effectively using a hybrid architecture. These policy constructs must be overcome if the system is to be beneficial and effective.

To understand the legal and policy obstacles preventing implementation, it was necessary to break down the components of hybrid architecture and examine each individually to determine whether legal and policy barriers inhibit the use of hybrid architecture support during USSF missions.

Given the complexity of the analysis and the numerous elements involved, the research team created a custom analytic framework to assess policy and legal risks and impacts.

The framework is based on a hybrid architecture notional model, where hybrid architecture characterization is composed of X% **USG systems,** Y% **commercial capabilities**, and Z% **international** solutions. Each of those three main components contain a mix of elements that in total comprise a Hybrid Architecture Model as depicted in Figure 3.

[5] Secretary of the Air Force Public Affairs. (2024, April 10). To Maintain Supremacy, Saltzman Unveils Strategy for Tighter, More Immersive Collaboration with Space Industries. United States Space Force. https://www.spaceforce.mil/News/Article-Display/Article/3737638/to-maintain-supremacy-saltzman-unveils-strategy-for-tighter-more-immersive-coll/.

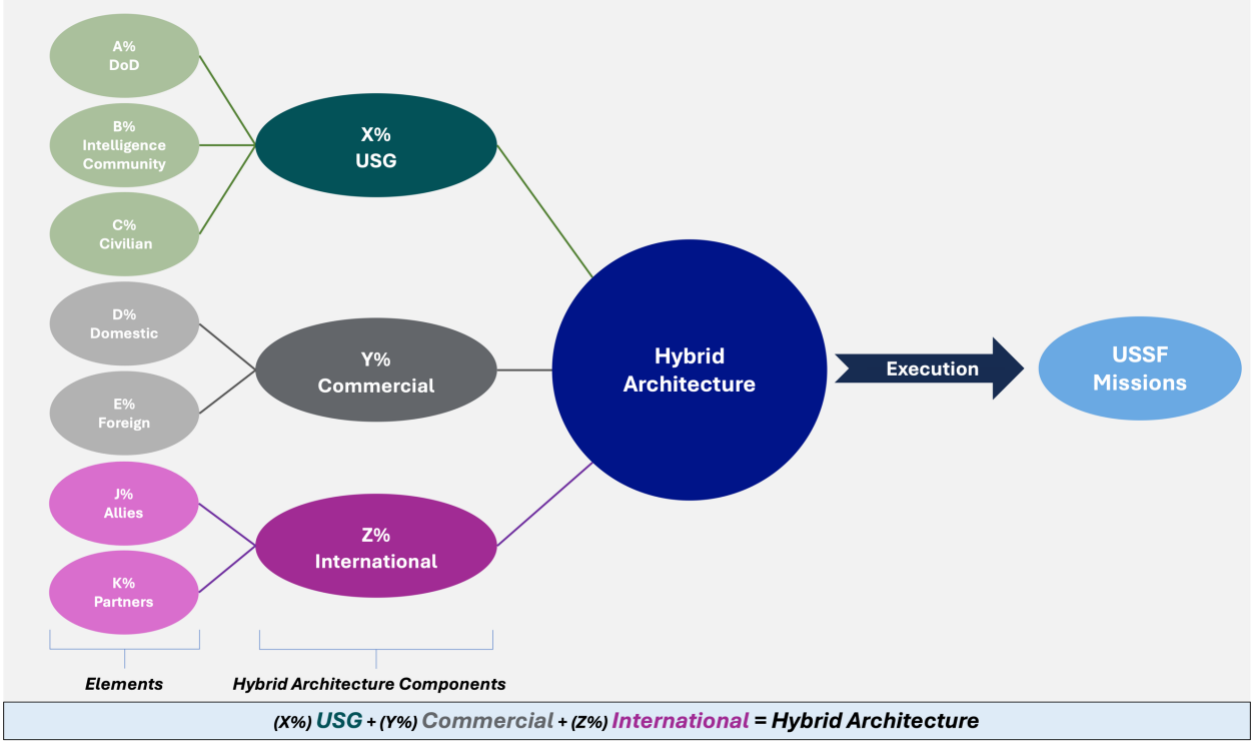

Figure 3. Notional Model of Hybrid Architecture for USSF Missions

The USG component is comprised of elements from DoD, IC, and civil agency systems, all of which can be called upon to execute priority missions. Commercial capabilities, as defined in the section Component Ownership can be either foreign or domestic elements. The international component is comprised of distinctly different elements of formal allies or in case-by-case partnerships.

This framework can encompass cost, schedule, or performance considerations for specific missions, which may be beneficial for future studies. For analytic purposes, this study did not consider the "ideal" mix, only that a hybrid architecture enables the execution of multiple USSF missions across a spectrum of ownership models. The components leveraged from a hybrid architecture can and will change to meet mission needs. Optimizing for the efficient, timely operational success of these missions is an objective enabled by a hybrid system.

Design Reference Mission (DRM) Impacts

DRM enablers provide support capabilities crucial to the success of a given mission. A DRM can be applied in multiple ways and across multiple mission sets. For this analysis, operational success was based on whether a DRM enabler could support a selected mission set. Selecting exemplary missions allowed the team to identify the legal and policy barriers to mission success.

For example, a Space Traffic Management (STM) mission that supports Space Domain Awareness and Space Superiority activities can be executed with primarily commercial and open-source solutions. This mission has been assigned to the Commerce Department, where it can be implemented commercially, though it has not been implemented yet. Other missions, such as Find, Fix, and Track (FFT) and Targeting (both kinetic and non-kinetic) also depend on core USSF DRM

enablers for mission success. Figure 4 depicts these missions and how they notionally align to the DRMs of SATCOM, TacSRT, and Space Control.

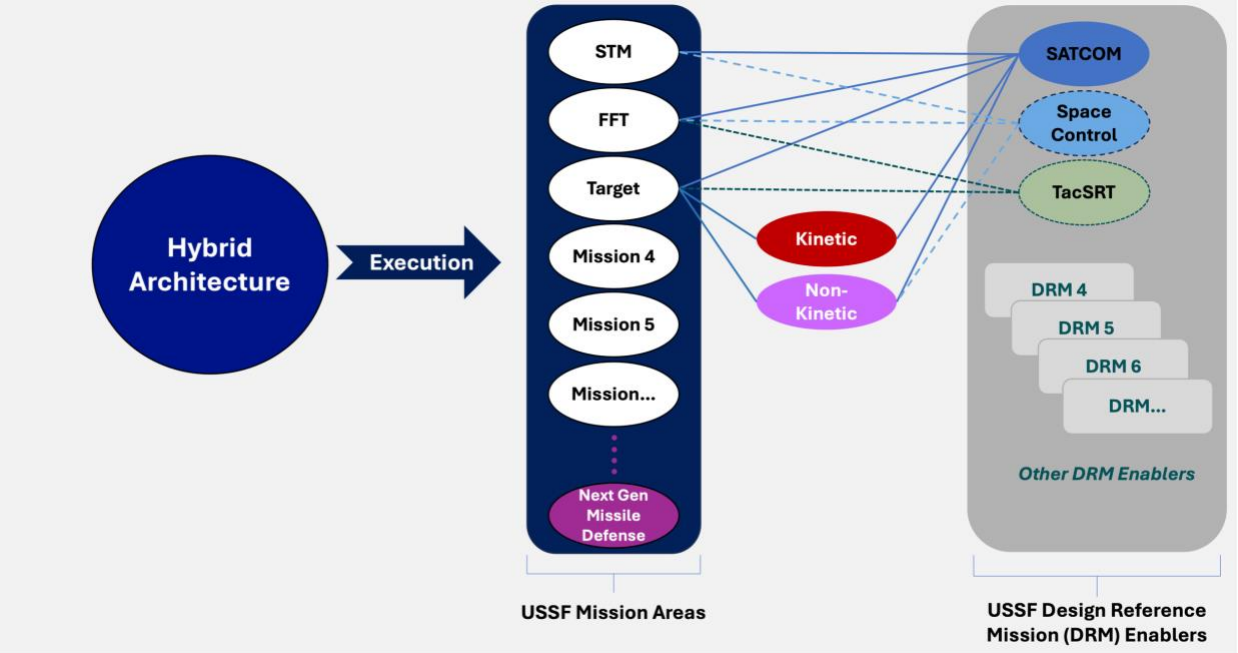

Figure 4. Conceptual Portrayal of Hybrid Architecture for Space

The DRM enabler exemplars of SATCOM, Space Control, and TacSRT and missions such as STM, FFT, and Targeting were selected because they span the mission set of the target architecture. They represent both USG capabilities (e.g., Kinetic and Non-Kinetic Targeting) and commercial needs (e.g., STM). They also include mission sets where foreign partners and allies may contribute (e.g., tracking).

All USSF hybrid architecture missions use DRMs, whether in some combination of the exemplar DRM enablers of SATCOM, TacSRT, and Space Control, or any number of *other DRMs* not explicitly assessed in this report. The missions and DRMs selected span the spectrum of hybrid architecture objectives in order to illuminate a range of barriers that should be addressed to increase the effectiveness of a USSF hybrid architecture.

USSF and DoD missions outside the hybrid architecture sphere, like ***Next Generation Missile Defense,*** also employ DRM enablers, where operational impacts from policy and legal issues may arise. The analytic framework may assist in evaluating these programs, as well.

Figure 5 demonstrates the full framework by visualizing the integration of the model with the exemplary missions and DRM enablers and highlighting key legal and policy barriers. This is the analytic framework used to identify the impactful legal and policy constraints and enablers.

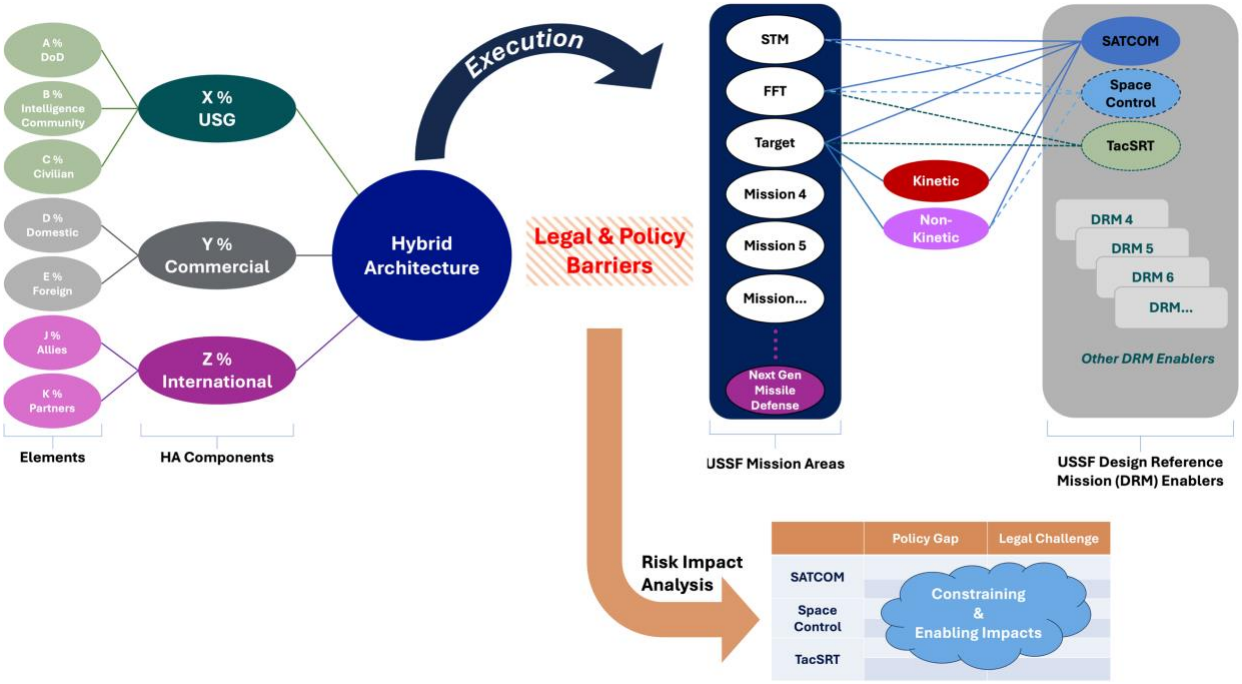

Figure 5. Analytic Framework for Hybrid Architecture Study

The analytic framework considers three primary dimensions:

1. Ownership of components in hybrid architecture
2. Mission applications via DRMs that enable successful hybrid architecture operations
3. A characterization of policy and legal barriers

Along these dimensions, the framework offers a way to identify barriers stemming from legal and policy requirements. It also helps assess the risks and barriers that are the focus of this study, as identified in the section: Initial Application of the Analytic Framework.

COMPONENT OWNERSHIP

Ownership is one of the primary dimensions of consideration in a hybrid architecture system. Hybrid architecture systems are comprised of components and assets owned by the USG, commercial entities, international allies, or partners**.** Blended systems will also contribute to the makeup of a hybrid architecture and, as such, should be accounted for when analyzing the approach. Just as government or commercial systems could be owned by the United States or partners, blended systems can be made up of any combination of the four options, **US government-owned, US commercial-owned, international government-owned, or international commercial-owned** (see Figure 6).

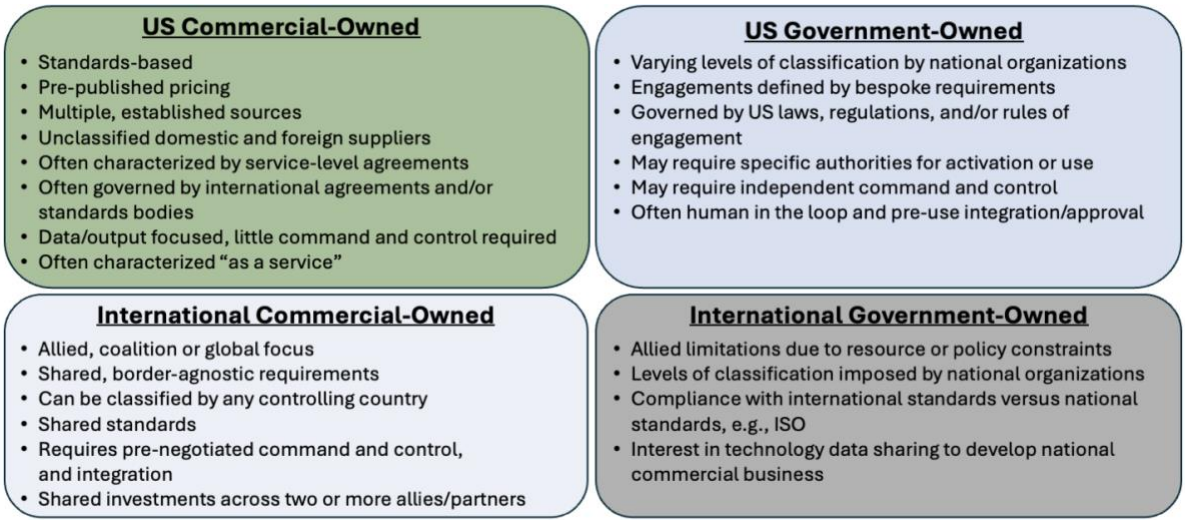

Figure 6. Program Type Characteristics

Government-owned systems refer to any capability, system, or product—including software, hardware, or algorithm—that is owned and controlled by a government through acquisition and whose employment within any architecture, hybrid or otherwise, is determined by the government owner. Government-owned systems may be owned by the United States or owned by a partner nation. Where necessary, the study made this distinction for completeness.

Government-owned systems may also be operated by government personnel or contractor personnel hired by the government. The study made no distinction between the two in the definition of a government-owned system. If a government has procured a system and makes decisions as to its use, the research team declared that system to be government-owned.

Commercial systems refer to a capability, system, or product—including software, hardware, or algorithm—which is owned by a commercial company.[6]

For purposes of this report, the team simplified the definition of a commercial system to focus on two core elements—ownership and decision-making. If any system is owned by a commercial entity that makes final decisions regarding employment, the system is commercial. These systems may be developed and owned by US companies or by non-US companies. Where necessary for study completeness, the research team made this distinction.

Commercial systems can be domestic or foreign; and their employment within an architecture, *hybrid or otherwise,* is determined by the commercial owner. Commercial systems are typically provided via contracts for specified services. These contracts typically also define the command and control of commercial sensors.

The need to incentivize commercial and international partners to join and support a hybrid architecture system is beyond the scope of this study but is addressed in a forthcoming paper from the Potomac Institute for Policy Studies.

[6] This designation does not apply to systems whose components may be commercially procured but are integrated into a government-owned system.

While the Space Force has multiple potential DRM enablers, this study focused on three:

Satellite Communications (SATCOM) is a vital capability using satellite constellations to provide secure, global, and beyond-line-of-sight communication for military operations, enabling command and control, space data transport, and tactical support to forces.

The Space Force is moving to evolve SATCOM from disparate systems into a single, resilient enterprise across all orbital regimes, capable of operating in contested environments to maintain information advantage for warfighters.

For this mission, the study focused on tactical and operational communications. It did not address strategic communications, and explicitly avoided discussion of nuclear command, control, and communications requirements, assuming those are reserved for USG only and not considered for hybrid architecture applications.

Tactical Surveillance, Reconnaissance, and Tracking (TacSRT) is a USSF-established online marketplace connecting commercial vendors with the Combatant Commands to rapidly deliver commercial, unclassified sensing and analytics products.

The TacSRT mission is to provide warfighters with timely, data-driven insights derived from commercial satellite data and other sources. This enables them to ask specific questions and receive detailed analytic products to support operational planning and decision-making.

Key aspects of the TacSRT mission include rapid response, leveraging commercial partners, using unclassified and releasable products to enhance multinational collaboration and fill intelligence gaps. TacSRT is becoming a Space Force initiative to complement traditional intelligence solutions.

Space Control, as defined by the USSF, includes the activities required to contest and control the space domain. The desired goal of Space Control is *space superiority*, a degree of control that allows forces to operate at a time and place of their choosing without prohibitive interference from space or counterspace threats, while also denying the same to an adversary.

Space Control consists of offensive and defensive counterspace operations conducted across space, electromagnetic spectrum, and ground segments of the space architecture (adapted from the USSF's *Space Warfighting*, 2025).[7] There is particular potential for commercial and international solutions in Space Domain Awareness—the timely, relevant, and actionable understanding of the operational environment. Space Domain Awareness is a critical factor that enables Space Control.

[7] United States Space Force. (2025). *Space Warfighting: A Framework for Planners*.

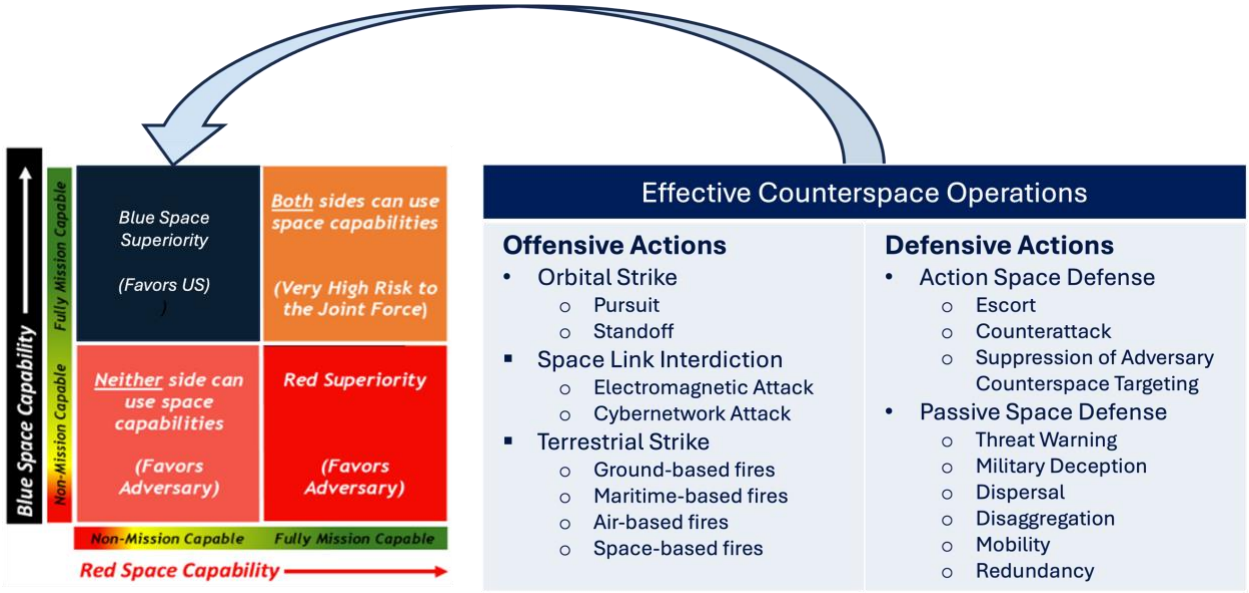

Figure 7. Space Control Elements[8]

These three mission enablers (SATCOM, TacSRT, and Space Control) vary considerably within this overall discussion. From the standpoint of commercial content, overall classification, and ease of implementation, they span almost the entire spectrum of consideration.

By virtue of their requirements and the maturity of the current space marketplace, both SATCOM and TacSRT are predominantly commercial. That said, government systems do exist and could be blended with commercial constellations to support mission success.

Space Control, however, is almost exclusively governmental in nature. There is no obvious commercial market for Space Control capabilities. While select commercial companies enact aspects of Space Control, decision-making remains inherently governmental and the study categorized these capabilities as government during analyses.

Operational Considerations

To function in a data-centric hybrid architecture, two key operational considerations must be factored into the system: *interoperability* and *network integration*. If systems cannot interoperate or network efficiently, the entire hybrid structure is affected (see Operational Consideration Example, on the next page).

Interoperability: The error-free interaction of systems at basic hardware or software levels is a key element of any hybrid system. Vital operational considerations for a hybrid system will include whether all systems interoperate seamlessly: Have they been designed and implemented to international standards agreed and adhered to by all parties? If systems are not interoperable, and need to be, what is the process to ensure interoperability?

[8] Elements of this graphic adapted from *Space Warfighting: A Framework for Planners* (March 2025).

Network integration: System integration is another operational consideration critical to the success of hybrid architecture. Integration requires computer systems to communicate at the machine level without human intervention. If they do not speak the same digital language, this cannot occur.

Operational Consideration Example

The current SATCOM environment in LEO is a good example of operational considerations.

The Starlink commercial capability from SpaceX *is not* interoperable with the US Title 10 tactical communications layer in development by the Space Development Agency, without the cumbersome use of in-space or terrestrial translator nodes. This is despite Space Development Agency optical and networking standards being adopted by international partners, and an interoperability validation facility established for those standards.

As SpaceX transitions to StarShield for government applications, how will interoperability be ensured? As Amazon LEO and other new commercial capabilities come online, will they be any more interoperable than their predecessors?

If these elements cannot interact with each other, they cannot be integrated into a fully functional hybrid architecture in times of conflict.

An interoperable, network-integrated hybrid architecture, which includes commercial and allied elements, raises new challenges. For example, *how does the traditional concept of Command and Control apply in a hybrid architecture?* Can the owner, employees, and/or board of directors of a commercial system deny government use during conflict. Similarly, can an ally or partner deny use of their governmental systems during conflict based on their own national priorities? *If traditional Command and Control may break down in hybrid applications, it begs the question: "If the Commander does not have control, do they have full command? "*[9]

Operational considerations are not the only barriers that face a hybrid architecture system. Other barriers can include organizational precedents, cultural issues, national and international priorities, among others. Such barriers lie beyond the scope of this report, and so were classified as "other."

RISK ANALYSIS

Not all of the barriers posed by a hybrid architecture will become risks or vulnerabilities. Understanding where these barriers pose risks, and understanding the level of risk they pose, is critical to being able to properly triage and address the most significant challenges.

Identification and management of risks and barriers in hybrid architecture applications is a continuous process. USG agencies, allies, partners, and commercial industry may differ in the prioritization of risks. As such, assessments should be continually reevaluated, revised, and reapplied as potential risks and risk prioritizations shift.

[9] The Defense Production Act of 1950, Pub. L. No. 81–774, 50 USC (1950). https://www.congress.gov/crs-product/R43767.

Risks are commonly characterized by likelihood and severity. A program identifies risks by identifying what can go wrong, exploring difficulties in program development, or identifying areas where information is lacking. Risk analysis focuses on both the *likelihood* and *severity* of the risk.

Figure 8 shows a notional Space Control risk matrix from a DoD operational perspective. While the DoD uses the term "consequence," the research team used the term "severity" since the immediate consequences of a barrier for hybrid architecture remain unclear.

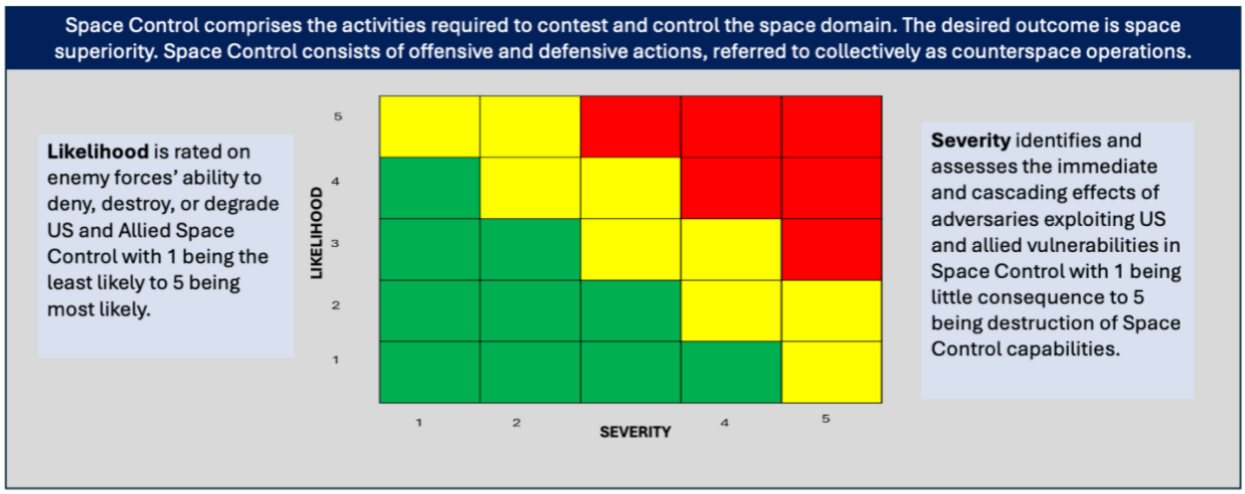

Figure 8. Notional Space Control Risk Matrix—Operational Perspective

Risk Mitigation

Once risks, like those facing hybrid architecture are identified, the next step is to mitigate those risks. Risk mitigation focuses on addressing risk: ensuring risk mitigation plans are feasible and affordable, and allowing adequate time to develop and implement the risk mitigation plan. Mitigation efforts must also assess the impact of risk mitigation plans on the overall schedule and technical performance of the system. In this way, programs can ensure their risk and mitigation expectations are realistic given program circumstances, constraints, and objectives.

Four strategies can lower or mitigate risks—accept, avoid, transfer, or control:

1. **Accept**: By accepting the risk, the program acknowledges that the risk event or condition may be realized, and the program is prepared to accept the consequences. The program should continue tracking the risk to ensure its likelihood does not increase and the accepted consequences do not worsen. Monitoring includes a continuous process to systematically track and evaluate the performance of risk mitigation plans.

2. **Avoid:** Through risk avoidance, a program reduces or eliminates the risk by taking an alternate path. It eliminates the source of the risk and replaces it with another solution.

3. **Transfer:** Risk transfer includes reassigning or delegating responsibility for tasks to mitigate a risk to another entity. Risks may be shared across multiple government organizations. However, programs should recognize transference of risk does not eliminate all responsibility. Risks must still be monitored for potential consequences.

4. **Control:** Risk control seeks to actively reduce risk to an acceptable level. Control generally entails taking action to reduce the likelihood or consequence of a risk to as low as practical, minimizing potential impacts. It assesses how the risk has changed and whether risk mitigation plans are working, or if additional actions should be taken to mitigate or control the risk.

More information about the risks related to hybrid architecture, as well as ways they may be mitigated, can be found in the sections: Examining and Mitigating US Risks in Hybrid Architecture and Findings and Recommendations.

The analytic framework above allows identification of risks generated by policy and legal barriers by exploring specific missions executed using hybrid architecture. This framework can also be adapted to model and understand how risks would change in a given hybrid architecture scenario with different mission objectives.

In its initial application, the framework revealed important risks to operations using hybrid architecture, as detailed in the next section.

INITIAL APPLICATION OF THE ANALYTIC FRAMEWORK

This section uses the analytic framework above to consider the impact of legal and policy risks on mission execution in a hybrid architecture, then evaluates them in terms of likelihood and severity. It first explores legal and policy barriers to creating a hybrid architecture framework, before assessing the mid- and long-term risks posed to US, commercial actors, and allies and partners. The risks are characterized by DRM enabler and system ownership (US, commercial, or allies and partners).

BARRIER IDENTIFICATION

The research team took a four-phase approach to identifying barriers stemming from legal and policy documents, using a custom database of 389 distinct laws, policies, and major geopolitical events related to hybrid architecture spanning 1950 through 2025.

Of the 389 database entries surveyed,103 were identified as directly relevant to one or more of the DRM enablers—SATCOM, TacSRT, and Space Control.

In phase two, laws, policies, and events were classified as either enabling or constraining factors for their DRM enablers. This yielded 79 enabling factors and 24 constraining factors; given the study's focus on risk, the enabling factors were subsequently excluded.

The eight key enabling laws and policies, listed below, demonstrate the breadth of space policy and laws across multiple decades and administrations:

1. 1950 Defense Production Act[10]
2. 1958 Executive Order 10789: Authorizing Agencies of the Government to Exercise Certain Contracting Authority in Connection with National-Defense Functions and Prescribing Regulations Governing the Exercise of Such Authority[11]
3. 1970 National Security Decision Memorandum 72: Exchange of Technical Data between the United States and the International Space Community[12]
4. 1984 Competition in Contracting Act[13]
5. 1991 National Space Policy Directive 3: US Commercial Space Policy Guidelines[14]

[10] The Defense Production Act of 1950, Pub. L. No. 81–774, 50 USC (1950). https://www.congress.gov/crs-product/R43767.

[11] Executive Office of the President of the United States. (1958). *Executive Order 10789: Authorizing Agencies of the Government to Exercise Certain Contracting Authority in Connection with National-Defense Functions and Prescribing Regulations Governing the Exercise of Such Authority* (ex). Office of the Federal Register, National Archives and Records Administration. https://archives.federalregister.gov/issue_slice/1958/11/15/8897-8900.pdf.

[12] National Security Council. (1970). *National Security Decision Memorandum 72: Exchange of Technical Data between the United States and the International Space Community*.

[13] United States 98th Congress. (1984). *Competition in Contracting Act of 1984*. https://www.congress.gov/bill/98th-congress/house-bill/5184.

[14] The White House. (1991). *National Space Policy Directive 3: U.S. Commercial Space Policy Guidelines*. https://csps.aerospace.org/sites/default/files/2021-08/Commercial%20Space%20Policy%20Guidelines%20Feb91.pdf.

6. 1994 Presidential Decision Directive/NSC-23: US Policy on Foreign Access to Remote Sensing Capabilities[15]
7. 1996 10 US Code § 9514 - Indemnification of Department of Transportation for losses covered by defense-related aviation insurance[16]
8. 2025 Executive Order 14369: Ensuring American Space Superiority[17]

In phase three, the 24 constraining factors were investigated to: 1) determine whether each constraint was legal or policy based, 2) identify the individual barriers each posed to hybrid architecture, and 3) categorize those barriers as either operational or other. This phase identified 63 distinct barriers emerging from legal and policy documentation.

Phase four combined a thematic analysis of the 63 individual barriers with interview data to produce 24 broader types of barriers as they apply to SATCOM, TacSRT, and Space Control (see Table 1).

[15] The White House. (1994). *Presidential Decision Directive/NSC-23: U.S. Policy on Foreign Access to Remote Sensing Capabilities*.

[16] Indemnification of Department of Transportation for Losses Covered by Defense-Related Aviation Insurance, Pub. L. No. 104–201, 10 USC (1996). https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section9514&num=0&edition=prelim.

[17] Executive Office of the President of the United States. (2025b). *Executive Order 14369: Ensuring American Space Superiority*. Office of the Federal Register, National Archives and Records Administration. https://public-inspection.federalregister.gov/2025-23845.pdf.

DRM	Barrier Type	Policy Themes	Legal Themes
SATCOM	Operational	n/a	• Data fidelity* • Risk of outdated technologies threatening interoperability • Unpredictable debris tracking capabilities and management • Data and platform vetting requirements slowing mission speed • Outdated technologies threatening mission capability
	Other	n/a	• Classification issues limiting information sharing • Licensing and regulatory requirements raising costs of cooperation
TacSRT	Operational	n/a	• Proliferated environment increasing collision risks • Proliferated environment increasing data fidelity risks, particularly from older assets • Limitations on data access and use creating barriers to commercial involvement • Limitations on data sharing slowing missions in hybrid environments • Loss of tactical custody and tasking latency increasing collision risks
	Other	• Notification requirements slowing mission execution	• Domestic controls on technology ownership and technology sharing increasing costs of cooperation • Data access validation issues limiting cooperative potential
Space Control	Operational	• National decision authorities limiting/slowing execution of time-critical missions	• Lack of integration and interoperability mandates • Dual-use technology restrictions impeding cooperation between US commercial and non-US • Debris avoidance needs reducing freedom of maneuver
	Other	• Transparent management of space assets can allow adversaries to gain critical knowledge of intent and capabilities • Approval/notification dynamics limiting/slowing execution of time-critical missions	• Classification issues • Licensing and regulatory requirements limiting technology and information sharing • Fidelity of commercial data creating liability issues and potential sources of insider threat

*Includes pedigree, accuracy, consistency, and availability

Table 1. Overall Policy and Legal Barrier Types to Hybrid Architecture by DRM

RISK ASSESSMENT

To the potential risk of these barriers, the research team assessed both the likelihood and severity of different barrier types. The likelihood of barriers to occur is based on asset ownership type: owned by the United States, owned commercially, or owned by allies and partners. The study used a 5-point

Likert scale to assess likelihood.[18] A single number was chosen for each entry based on subject matter expert (SME) evaluation of preponderance of evidence and experience.[19]

The research team similarly scored the severity of barriers, should they occur, if laws and/or policies are not changed. Severity scoring was based on consequences according to asset ownership type: owned by the United States, owned commercially, or owned by allies and partners. As above, the team used a 5-point Likert scale to assess severity[20] and a single number was chosen for each entry based on SME evaluation of preponderance of evidence and experience.[21]

For each ownership type, the research team also assessed severity for both mid-term (18 months to 5 years) and long-term (5+ years) timeframes. This approach provided initial insight into whether the severity of each barrier increases over time to provide a preliminary look at potentially high risks to mission.

To assess risk levels, the likelihood and severity scores for each barrier type were combined to produce a risk-scoring matrix. Barriers were classified as either low risk (green cells), moderate risk (yellow cells), or high risk (red cells). The research team also determined risk levels for both the mid-term and long-term time horizons across each type of asset ownership—US, commercial, and allies and partners.

The risk-scoring matrix in Table 2 provides the team's preliminary assessment of mid- and long-term risks each barrier type poses to participation in a hybrid space architecture for the US, commercial, and allies and partners. Barriers are presented by DRM enabler and classified as either operational or other in nature. It is based on the initial qualitative analysis of the laws and policies examined. However, generalizing these results beyond the scope of this study requires a more comprehensive analysis.

[18] The likelihood ranking for the Likert scale was setup as 1 = Extremely Unlikely, 2 = Unlikely, 3 = Neutral, 4 = Likely, 5 = Extremely Likely.

[19] Table 5 provides a breakdown of the likelihood scoring.

[20] The severity ranking for the Likert scale was setup as. 1 = No Impact, 2 = Minor Impact, 3 = Moderate Impact, 4 = Major Impact, 5 = Severe Impact.

[21] Table 6 in provides a breakdown of the severity scoring.

DRM	Type	Barrier Theme	Unmitigated Risk (Likelihood x Severity)					
			US		Commercial		Allies & Partners	
			Mid-term: *18 mo. to 5 yrs.*	Long-term: *5+ yrs.*	Mid-term: *18 mo. to 5 yrs.*	Long-term: *5+ yrs.*	Mid-term: *18 mo. to 5 yrs.*	Long-term: *5+ yrs.*
SATCOM	Operational	Data fidelity*						
		Risk of outdated technologies threatening interoperability						
		Unpredictable debris tracking capabilities and management						
		Data and platform vetting requirements slowing mission speed						
		Outdated technologies threatening mission capability						
	Other	Licensing and regulatory requirements raising costs of cooperation						
		Classification issues limiting information sharing						
TacSRT	Operational	Proliferated environment increasing collision risks						
		Proliferated environment increasing data fidelity risks, particularly from older assets						
		Limitations on data sharing slowing missions in hybrid environments						
		Loss of tactical custody and tasking latency increasing collision risks						
		Limitations on data access and use creating barriers to commercial involvement						
		Domestic controls on technology ownership and technology sharing increasing costs and risks of cooperation						
		Data access and validation issues limiting cooperative potential						
	Other	Notification requirements slowing mission execution						
Space Control	Operational	Lack of integration and interoperability mandates						
		Dual-use technology restrictions impeding cooperation between US commercial and non-US						
		Debris avoidance requirements reducing freedom of maneuver						
		National decision authorities limiting/slowing execution of time-critical missions						
	Other	Licensing and regulatory requirements limiting technology and information sharing						
		Fidelity of commercial data creating liability issues and potential sources of insider threat						
		Classification issues						
		Transparent management of space assets can allow adversaries to gain critical knowledge of intent and capabilities						
		Approval/notification dynamics limiting/slowing execution of time-critical missions						

*Includes insider and cyber threats and data pedigree

Table 2. Mid-Term and Long-Term Risk Levels for Barriers by DRM and Asset Ownership

EXAMINING AND MITIGATING US RISKS IN HYBRID ARCHITECTURE

After conducting this preliminary analysis, several barriers emerged as potentially high risks for the US in both mid- and long-term.[22] These high-risk barriers shed initial light on policy and legal priorities for the US to address.[23] They are presented below in Table 3, sorted by DRM enabler:

DRM Enabler	High-Risk Barriers to US (in both Mid-Term and Long-Term)	Barrier Type
SATCOM	Outdated technologies threaten mission capability.	Operational
	Classification issues limit information sharing.	Other
TacSRT	Loss of tactical custody and tasking latency bring products and services to the warfighter late.	Operational
	Domestic controls on technology ownership and technology sharing increase costs of cooperation.	Operational
Space Control	Integration and interoperability mandates are lacking.	Operational
	Limited and non-standardized on-orbit logistics and debris avoidance requirements reduce freedom of maneuver.	Operational
	Fidelity of commercial data creates liability issues and potential sources of insider threat.	Other
	Transparent management of space assets can allow adversaries to gain critical knowledge of intent and capabilities.	Other

Table 3. High-Risk Barriers for US in Both Mid- and Long-Term by DRM Enabler

The high-risk barriers in Table 3 emerge from the legal and policy documents surveyed in this analysis that either overregulate or underspecify aspects of US participation in a hybrid architecture. (A selection of these documents is presented in Table 4). This is not a comprehensive list; it shows the utility of the analytic framework and represents a starting point for future, in-depth analysis. This approach to risk assessment facilitates potential law and policy changes by identifying high-risk barriers and the specific laws or policies from which they emanate.

The limited barriers already found demonstrate the need for changes. This discovery forms the core of this study's **Finding 1: Dozens of laws, policies, and events pose potentially critical hurdles to hybrid architecture; all can be overcome.**

The analytic framework and risk analysis are tools policymakers might use to suggest changes via legislation like the National Defense Authorization Act, executive order, or other policy guidance vehicle (memo, regulation, instruction, etc.). Creating a task force to pursue such changes is the core element of **Recommendation 1: Remove critical legal and policy barriers by chartering a Hybrid Architecture Task Force to lead hybrid architecture baselining, barrier fact finding, and needed policy and legislative changes.**

[22] Of note, one operational barrier for the US in SATCOM (Risk of outdated technologies threaten interoperability) moves from moderate risk in the mid-term to high risk in the long-term.

[23] High-risk barriers are indicated by red cells in both time frames of Table 2).

Type	Preliminary List of US Laws and Policies Creating Risks	Reference
Law	Arms Export Control Act[24]	See Example 1
Law	Export Control Reform Act of 2018	See Example 1
Policy	US Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway[25]	See Example 2
Policy	Secretary of Defense Memorandum: Tenets of Responsible Behavior in Space	See Example 3
Policy	National Security Council 6108: Certain Aspects of Missile and Space Programs	See Example 4
Law	Extraordinary Contractual Actions and the SAFETY Act	See Example 5
Law	Commercial Remote Sensing	Sec 960.9B Sec 960.10A 2
Law	United States Code Title 51—National and Commercial Space Programs (Debris Avoidance)	Section 30701 A1
Law	Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005	Sec 914
Law	William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021	Sec 1607, Sec 1609
Law	National Defense Authorization Act for Fiscal Year 2022	Sec 1607
Law	National Defense Authorization Act for Fiscal Year 2024	Sec 1610
Policy	Department of Defense Instruction 3100.11: Management of Laser Illumination of Objects in Space	Whole document
Policy	United Nations General Assembly Resolution 77/41: Destructive Direct-Ascent Anti-Satellite Missile Testing	Whole document

Table 4. Preliminary List of Laws and Policies Creating Risks for the US

[24] Arms Export Control Act and the Export Control Reform Act of 2018, Pub. L. No. 90–629, 22 USC (2025). https://www.govinfo.gov/content/pkg/COMPS-1061/pdf/COMPS-1061.pdf.

[25] United States Department of Defense. (2022). *US Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway*. https://media.defense.gov/2024/Oct/26/2003571790/-1/-1/0/2024-06-RAI-STRATEGY-IMPLEMENTATION-PATHWAY.PDF.

SELECTED EXAMPLES OF SPECIFIC RISKS AND LEGAL MODIFICATIONS

Example 1

Modifications to laws, the Arms Export Control Act and the Export Control Reform Act of 2018, are required to enable US commercial dominance in remote sensing. Domestic controls on technology ownership and technology sharing inhibit cooperation with partners and allies. Industry is deterred from investing in requisite technologies due to potential risks on return, which is translated to high-risk operational vulnerabilities to TacSRT for the US. The Export Control Reform Act controls sharing with allies, foreign launch partners, and foreign-owned ground network. It should be noted, the November 2025 DoD Memorandum "Transforming the Defense Acquisitions System" and attached Acquisition Transformation Strategy is the latest reform attempt, but given its recency, has yet to demonstrate substantive impact.[26]

Specific Risks

1. Ambiguous export controls impede rapid sensor and small satellite production of units that use dual-use technology (e.g., optics, infrared, radar, radio frequency, propulsion, secure comms, algorithms, etc.).
2. Key intelligence, surveillance, and reconnaissance data cannot be shared within timelines relevant to the pace of contemporary operations and requisite threats. This issue and associated risks have existed and been acknowledged for decades, and some reforms have occurred.

Example 2

The 2021 US DoD Responsible Artificial Intelligence Strategy and Implementation Pathway needs refinement to resolve a policy rift between top-level messaging (as shown in White House Executive Order 14179: *Removing Barriers to American Leadership in Artificial Intelligence,*[27] and December 2025 SecWar guidance[28]) and operational implementation. The 2025 executive order is clear that AI/ML tools should be aggressively embraced, however the

[26] United States Department of War. (2025a). *Transforming the Defense Acquisition System into the Warfighting Acquisition System to Accelerate Fielding of Urgently Needed Capabilities to Our Warriors*. https://media.defense.gov/2025/Nov/10/2003819441/-1/-1/1/ACQUISITION-TRANSFORMATION-STRATEGY.PDF.

[27] Executive Office of the President of the United States. (2025a). *Executive Order 14179 Removing Barriers to American Leadership in Artificial Intelligence*. Office of the Federal Register, National Archives and Records Administration. https://www.govinfo.gov/content/pkg/FR-2025-01-31/pdf/2025-02172.pdf.

[28] United States Department of War. (2025b). *The War Department Unleashes AI on New GenAI.mil Platform*. https://www.war.gov/News/Releases/Release/Article/4354916/the-war-department-unleashes-ai-on-new-genaimil-platform/.

2021 guidance contains Five Tenets[29] that create onerous barriers to implementing AI/ML. This hinders adoption of cyber resilience, data tagging, anomaly identification, identity baselining, and incident response.

The requirement for contractors to address the Five Tenets laid out in the implementation plan mandates "comprehensive documentation of data sources and model development, robust bias detection and mitigation, regular security assessments against standards like NIST SP 800-53, and governance structures that maintain alignment with DoD AI Ethical Principles."[30] This increase in compliance and documentation requirements further complicates an already cumbersome acquisitions process and slows the procurement and integration of commercial capabilities.

Specific Risks

1. A risk-averse environment slows integration of modern commercial capabilities into DoD efforts.
2. Increased risk of network compromise exists, due to outdated data security tools.
3. Exclusion of needed allied and partner data slows decision-making.
4. Adversaries gain information advantage due to greater willingness to employ AI/ML and other advanced tools.[31]

Example 3

The Secretary of Defense Memorandum: Tenets of Responsible Behavior in Space ensconces policy directing "transparent management of space assets." This requires modification to enable space superiority, as the policy can allow adversaries to gain critical knowledge of intent and capabilities. If strictly adhered to, this can create operational vulnerabilities to Space Control. Notably, the memorandum's intent to "communicate and make notifications to enhance the safety and stability of the domain" risks exposing US offensive counterspace options to adversaries. As written, this policy guidance is misaligned

[29] The Five Tenets are: **Responsible** (design systems that serve intended purposes without causing unintended harm), **Equitable** (ensure systems function without bias across diverse populations and scenarios), **Traceable** (maintain transparency in how AI systems operate and make decisions), **Reliable** (develop systems that perform consistently under varying conditions), and **Governable** (design mechanisms for appropriate human intervention and control).

[30] Broadbent, R. A. (2025). DoD AI Compliance: Key Requirements and Strategic Implementation. *The National Law Review*, *XVI* (23). https://natlawreview.com/article/dod-ai-compliance-guidance-government-contractors.

[31] United States Office of the Secretary of Defense for Industrial Base Policy. (2025). *Artificial Intelligence (AI) in Defense: A Roadmap for the Future of the Defense Industrial Base (DIB)*. United States Department of Defense. https://www.businessdefense.gov/ibr/pat/docs/AI-and-the-DIB-Roadmap.pdf.

with the current administration's approach to rules of engagement for military operations. Alignment with current policy guidance can help ensure mitigation of operational risk.[32]

Specific Risks

1. The default status of the Tenets could inhibit full-spectrum space superiority training, exercise, and combat operations.
2. Policy guidance becomes misaligned with the current administration's approach to rules of engagement for military operations.

Example 4

National Security Council 6108 from 1961, requires revision to the section that states "any test which includes destroying a satellite or space vehicle shall not proceed without specific Presidential approval."[33] Space superiority is at risk without the option for comprehensive testing in space. This restriction goes beyond debris-generating destruction events to include tests that should not require that level of presidential approval, such as destructive cyber testing on a satellite or directed energy tests on an end-of-life satellite to assess survivability.

Specific Risks

1. Development timelines will balloon if explicit presidential approval is required for every test.
2. Organizations will become risk averse to developing capabilities that need to be tested in space.
3. Capabilities necessary to deter threats will not be tested and ready when needed.

Example 5

The 48 Code of Federal Regulations Part 50[34]—Extraordinary Contractual Actions and the SAFETY Act require modifications to account for the increased use of commercially-owned

[32] Executive Office of the President of the United States, 2025b.
[33] United States National Security Council. (1961). *Certain Aspects of Missile and Space Programs*. https://aerospace.csis.org/wp-content/uploads/2019/02/NSC-6108-Certain-Aspects-of-Missile-and-Space-Programs_fulldeclass.pdf.
[34] This section, also referenced in Federal Acquisition Regulation part 50 comprises the 1958 legislation PL 85-804 and the 2002 SAFETY Act.

assets in wartime.[35] Commercial assets used by the military may become military targets, causing commercial financial losses. In a hybrid architecture, financial risk is likely to center on loss of capital or income. However, "authority to approve requests to obligate the Government in excess of 90,000 USD may not be delegated below the secretarial level."

Within the Department of the Air Force, this authority "has been used mostly with respect to space launch and nuclear activities given the unique risks associated with those activities." However, the risk to commercial assets in war may rise to a similar level, so indemnification or government backed war-risk insurance may be necessary.

Specific Risks

1. The commercial provider may lose future revenue and investment capital due to kinetic or non-kinetic attack.
2. The commercial company will be unable to recoup the full value of lost assets if greater than 90,000 USD.
3. Requiring secretarial approval for such transaction can hinder commercial collaboration, development, and support.

This analysis is only an initial application of the framework advanced in this study; it offers a potential path forward for the USSF to assess and subsequently mitigate the legal and policy risks facing a successful hybrid architecture for space. However, a mature model, applied across different missions and DRM enablers, and validated through qualitative engagement with the USSF, would boost the utility and applicability of the model and increase confidence in the barriers identified through this method.

[35] Public law 85-804 lets the President permit department heads to indemnify contractors for losses incurred as a result of contract performance, in certain circumstances, but has only been implemented for the Department of Defense, and only with respect to risks defined in the contract as "unusually hazardous or nuclear in nature."

FINDINGS AND RECOMMENDATIONS

As has been detailed in this study report, the best way to provide the USSF with the speed, capacity, interoperability, and redundancy needed to deter and, if necessary, defeat our adversaries is through an effective hybrid architecture. The key findings and recommendations revolve around completing the pivot to a hybrid architecture as quickly and smoothly as possible.

The USSF is headed in the right direction in pursuing a hybrid architecture. However, the effort is not yet fully coordinated and integrated enough to truly succeed. Legal and policy barriers, both real and perceived, are slowing the adoption. This leaves the United States at risk and ill-prepared to deter conflict with adversaries like China, whose own hybrid architecture is advancing rapidly, uninhibited by such barriers.

By accelerating development of their own hybrid architecture, US adversaries have taken away the luxury of time. The earlier the United States identifies and mitigates the risks and barriers associated with the pivot to a hybrid architecture, the faster, smoother, and more effective the pivot will be. To that end, and with knowledge gained from this study, the research team offers the following findings and recommendations.

Finding 1: Dozens of laws, policies, and events pose potentially critical hurdles to hybrid architecture; all can be overcome.

Of 389 distinct discovered laws, policies, and precedent-setting geopolitical events related to hybrid architecture, dozens pose potentially critical hurdles. None are insurmountable.

Outdated statutes and policies, dating as far back as the 1950 Defense Production Act, will pose significant risks to implementing and accelerating hybrid architecture if they are not reviewed and revised.

The 2026 National Defense Authorization Act and recent Executive Orders such as "Ensuring American Space Superiority" (December 18, 2025) provide the direction, vision, and top cover required to expeditiously eliminate or revise antiquated and inconsistent bureaucratic policies. Nevertheless, significant senior leader attention as well as analysis and implementation effort will be required due to the number and scope of the needed changes and expected cultural resistance across the DoD and IC.

Recommendation 1: Remove critical legal and policy barriers by chartering a Hybrid Architecture Task Force to lead hybrid architecture baselining, barrier fact finding, and needed policy and legislative changes.

The USSF should charter a Hybrid Architecture Task Force, perhaps driven by the Chief of Space Operations' Strategic Initiatives Group. This group should baseline hybrid architecture and the barriers identified in this report, then aggressively pursue the policy changes needed to remove critical barriers and accelerate the hybrid architecture pivot.

The Task Force should be given a priority mission (e.g., Find, Fix, Track, Target, Engage, Assess [F2T2EA] or GMTI/AMTI) for kill chains, or space elements of Next Generation Missile Defense) to focus on near-term activity. The team should be tasked to baseline hybrid

architecture by maturing the Hybrid Architecture Model documented in this report, (i.e., 1) specify which elements of hybrid architecture need to provide specific capabilities to close F2T2EA or missile defense kill chains, and 2) include timelines and interconnections). Baselining enables the Task Force to identify, prioritize, and quarterback value-added policy revisions and propose needed legislative changes required to mitigate the critical legal and policy risks within 12 months.

The team would work with policy and legal experts, and industry associations such as the National Security Space Association and the SmallSat Alliance. The Task Force should also use AI tools and SMEs to delve deeper into the risks identified in this study and respond to additional inputs from the acquisition and operations communities as more risks and issues are discovered.

In conjunction with the hybrid architecture baselining, an initial "fact finding" phase should identify additional barriers and determine which require policy or legislative change. An educational program across DoD and IC elements can be undertaken to remove cultural barriers.

Without reforming the dozens of antiquated and inconsistent policies that pose critical barriers, the DoD and USSF risk failing to move quickly enough to deter China. A dedicated task force provides the best mechanism to quickly focus policy advocacy on the most significant barriers and drive necessary revisions.

Finding 2: USSF delays in fully adopting modern data-centric solutions could paralyze combat operations.

Antiquated, risk-averse mission data and cybersecurity postures hinder operations and slow adoption of modern tools to assure data fidelity.

Significant confusion and misinformation permeate both acquisition and operations as to the extent to which IC, civil, commercial, and international elements of the hybrid architecture can be "trusted" and/or used in combat operations. This confusion and resistance arise, in part, from insufficient exposure to and embrace of modern cyber and data-centric tools such as AI/ML. Treating data fidelity as a binary decision, that data arriving from sovereign systems can be trusted and other data cannot, creates false confidence and unnecessary "fog of war." The answer cannot be wider moats and higher walls that exclude critical information. Overall mission risk will often be reduced by accepting more data fidelity and cyber-attack surface risk to bring in commercial and allied data, with modern tools.

Cyber and insider threats can corrupt all data, so the best approach is to ingest and digest/process all available hybrid architecture data using modern tools within a zero trust framework.

Simplistically, two independent sensors, each with 90% assurance, are better than one sensor with 98% assurance; and statistically combining data from all three is the most robust approach. For example, within the positioning, navigation, and timing mission area, synthesizing all available multi-Global Navigation Satellite System (GNSS) and communications signals produces superior assurance to GPS M-code (a military-grade encrypted GPS signal), yet many platforms and weapons rely only on GPS.

While hybrid architecture data fidelity/integrity risks certainly exist and must be identified and managed, the risk of inaction or hesitation is greater. The USSF cannot wait for perfect modern data management tools. Instead, it must empower commanders to use the best tools they have and iteratively improve them over time. Moving out on hybrid architecture, despite imperfect tools and the fog of war, aids in resolving technical integration issues, archaic procedures and policies, misinformation, and change-averse cultural mindsets.

Recommendation 2: Mitigate data fidelity risks by embracing mission command, zero trust, and modern data and cyber tools.

Empower, task, and resource commanders to accelerate adoption of the hybrid architecture by acquiring and fully using IC, civil, commercial, and international data, starting today. Adopt a zero trust framework, with modern data management, cybersecurity, and processing tools and incorporate lessons from USTRANSCOM and at-scale commercial implementations.

Rigid and time-consuming steps such as traditional acquisition milestones, calibration, and "ops acceptance" are well intentioned but often counter-productive; they must be replaced by more continuous DevSecOps processes that allow all data and capabilities to be considered and to evolve over time. Some data will be more trusted than others. Over time, through operations and wargaming, commanders will master all elements of the hybrid architecture. Within the Space Domain Awareness mission area, for example, even the best sovereign sensors are not everywhere, seeing everything of interest, all the time, in real time. Including all hybrid architecture data as integral elements of the architecture is essential for timely and accurate operational decisions.

To do so, The USSF should embrace new technical tools to manage data complexity and achieve mission command objectives. Traditional zero trust techniques, such as Kalman filtering, can be combined with 21st century data management tools, such as structured data lakes mined by modern AI/ML engines. Experimentation and rapid iteration are key, within appropriate and clearly delineated mission command boundaries.

To quickly reap the benefits of and illuminate the potential barriers to implementing data-centric mission command across the USSF, consider starting with the GMTI/AMTI and TacSRT mission areas. Enable use of IC, civil, commercial, and allied remote sensing data across the operational target engagement process of F2T2EA. Emerging space-based GMTI and AMTI capabilities need to be integrated with TacSRT commercial and international capabilities to support kill chain operations. The superb integration observed in Operation Absolute Resolve needs to be routine, at scale, in the presence of peer threats, and on rapid planning timelines.

To facilitate data fidelity in the face of cyber threats, improved/increased cyber testing in space will be necessary. This involves creating realistic scenarios to find and fix vulnerabilities in satellites and ground systems, using real orbit tests, dedicated test satellites, digital cyber test ranges, simulating space environments; and focusing on autonomous defense, AI-driven detection, and developing new tactics against threats like

spoofing, jamming, and unauthorized commands. Cyber testing would expand wargaming events like "Hack-A-Sat" to move beyond just identifying attacks to proving defensive capabilities in orbit. In addition, there is a need to ensure that cyber testing is realistic and continuous throughout system lifecycles; while systems in sustainment may be static, the threats are constantly evolving. Many cyber risks remain undiscovered, and undiscovered risks cannot be mitigated and could paralyze combat operations.

USTRANSCOM recently implemented a very successful approach to moving war materiel with varying classified attributes across a transportation network that includes sovereign, commercial, and allied capabilities. Their experience and lessons learned could inform USSF's embrace of modern data-centric tools and architectures.

Successfully implementing mission command requires strong and continuing top cover from senior DoD and USSF leadership. Commanders empowered to accelerate the hybrid architecture will stumble and encounter anticipated and unanticipated risks and barriers. Senior leaders will need to provide legal and policy support to resolve barriers, and to continue to emphasize the importance of thoughtfully, deliberately, and quickly pivoting to hybrid architecture. For example, if a commander has questions about the conditions under which TacSRT commercial imagery can be used for targeting/attack, senior leaders must provide pertinent, supporting legal advice and promptly address any barriers.

CONCLUSION

Accelerating a full, smooth, and deliberate pivot to a hybrid space architecture is necessary and achievable, but not trivial. Risks and barriers to accelerating the hybrid architecture exist. They must be illuminated and carefully navigated. Deliberate effort will be required to revise antiquated policies and shift cultural predispositions. Nevertheless, delay or hesitation is the greater risk.

The DoD and USSF already have most of the legal and policy tools required to begin implementing the recommendations and are well equipped to advocate for any legislative changes. As the hybrid architecture vision is implemented, the deterrence and warfighting benefits will quickly accrue and outweigh any additional risks and barriers that emerge. Accelerating effective hybrid architecture is necessary, but not sufficient preparation for space warfighting.

A unifying thread through the findings and recommendations is that to preserve peace, the USSF must prepare the hybrid architecture for war. As the Roman writer Vegetius asserted, "Si vis pacem, para bellum." (If you want peace, prepare for war.) **The DoD and USSF must *prudently and deliberately* double down on the hybrid architecture with speed, but also with coordination, integration, and synchronization to ensure potential barriers are proactively resolved and expected mission benefits—peace through strength—are realized across the enterprise**.

APPENDIX A: ACRONYMS

AFA	Air and Space Forces Association
AI/ML	Artificial Intelligence and Machine Learning
AMTI	Air Moving Target Indicator
CASR	Commercial Augmentation Space Reserve
DevSecOps	Development, Security, and Operations
DoD	Department of Defense
DRM	Design Reference Mission
F2T2EA	Find, Fix, Track, Target, Engage, Assess
FFT	Find, Fix, and Track
GMTI	Ground Moving Target Indicator
GNSS	Global Navigation Satellite System
GPS M-code	Global Positioning System Military Code
IC	Intelligence Community
LEO	Low Earth Orbit
NATO	North Atlantic Treaty Organization
NSSE	National Security Space Enterprise
SATCOM	Satellite Communications
SME	Subject Matter Expert
STM	Space Traffic Management
TacSRT	Tactical, Surveillance, Reconnaissance, and Tracking
US	United States
USG	United States Government
USSF	United States Space Force
USSPACECOM	United States Space Command
USTRANSCOM	US Transportation Command
WAS	Warfighting Acquisition System

APPENDIX B: RESEARCH METHODOLOGY

The research team employed a three-stage research design consisting of multiple methods to explore legal and policy risks to hybrid architecture for the space domain and to inform recommendations on implementing an effective hybrid architecture (see Figure 9).

Stage 1 filtered legislative and policy history to identify the 389 potential legal and policy barriers and to develop the analytic framework of the paper. These two elements form the heart of this study.

Stage 2 used that analytic framework to conduct a preliminary risk analysis that relied on a multi-method approach of quantitative document analysis and qualitative interview analysis. The team also created a case study on the Commercial Augmentation Space Reserve (CASR), which will be detailed in a forthcoming paper.

Stage 3 subjected the risk analysis findings to an external validation process through dedicated Red Team workshops and a series of panel discussions with a Technical Advisory Team.

From external validation, the research team developed recommendations.

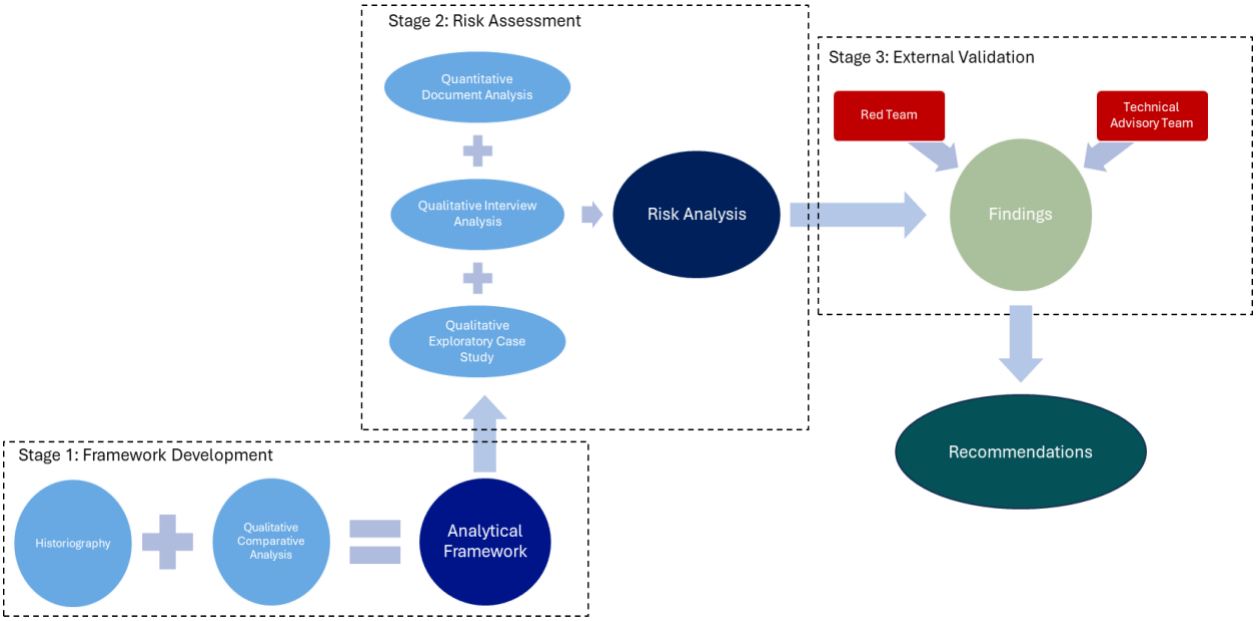

Figure 9. Three-Stage Research Design

Stage 1: Development of the Analytic Framework

As a major data collection effort for developing the analytic framework, the research team created a ***custom Potomac Institute database*** of 389 distinct policies, laws, international dynamics, and major geopolitical events relevant to hybrid architecture for space. The database covers public, open-source documentation, and information from 1950 through 2025. Researchers catalogued each entry in the database according to the originating level of government (US DoD, US non-defense agency, US interagency, US national level, international), the type of source (i.e., executive orders, legislation, doctrine, treaties, events, etc.), and the relevance to SATCOM, TacSRT, and Space

Control. This database is the first of its kind, as no such database currently exists in the public domain.

The research team also undertook a targeted literature review of prior studies related to hybrid architecture and collected data on five USG Programs of Record with characteristics similar to a hybrid architecture for space.

From this data collection, the research team utilized historiographical methods and qualitative comparative analysis to create the analytic framework. Through historiography, the team assessed the historical policy context and roles, missions, and responsibilities of the USG related to a hybrid architecture for space.

Stage 2: Risk Assessment

Stage 2 of the research methodology focused on an initial application of the analytic framework. Data collection in Stage 2 built on Stage 1 to include two additional avenues of data collection:

1. Semi-structured interviews with external subject matter experts (SMEs)
2. Unstructured interviews with SMEs, obtained through event attendance and snowball sampling

The research team conducted 14 semi-structured SME interviews and 12 unstructured SME interviews. The **total of 26 SME interviews** exceeded the team's expected minimum of 20 interviews. All individuals requested non-attribution in the project. The research team classified these 26 interviewees based on their experience into 1 of 5 categories: 1) Policy, 2) Legal, 3) Technical, 4) Commercial, and 5) Operational. See Figure 10 for a breakdown of interviews per category. The research team created these categories to mitigate bias and increase inferential response validity.

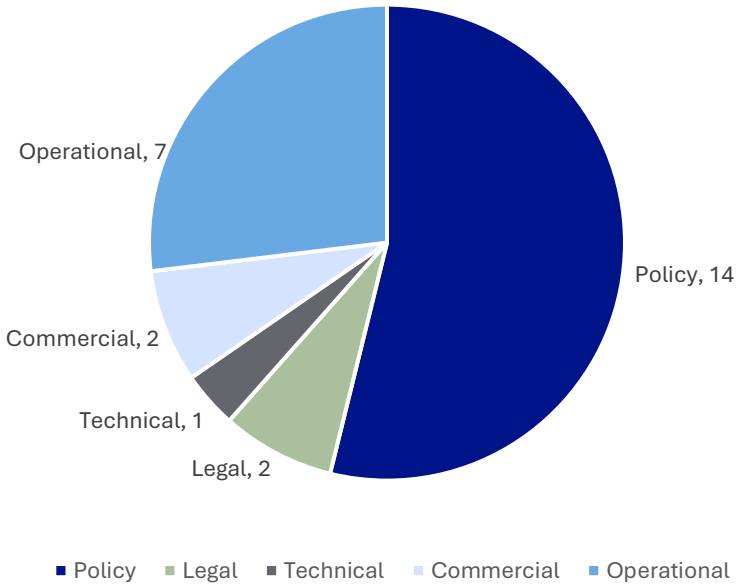

Figure 10. Breakdown of Targeted Interviews by Number and Expertise

To facilitate data collection through interviews, the research team attended three events: the Space Defense and Security Summit, the Air and Space Forces Association (AFA) National Convention, and Rethinking Strategic Competition in Space hosted by Lawrence Livermore National Lab. These events provided key contextual information for developing and framing research questions and enhanced snowball sampling of interview subjects by providing contacts and referrals.

Multi-Method Analysis

Figure 11 provides an overview of the research team's multi-method approach to assess risks and obtain findings. The multi-method approach for risk assessment consisted of document analysis, interview analysis, and an exploratory case study. Document analysis occurred in two steps, with the interview analysis supporting the subsequent likelihood, severity, and risk scoring.

Document Analysis: In the first round of document analysis, the research team took a four-phase approach to identifying barriers stemming from legal and policy documents using the team's custom database of laws, policies, and events related to hybrid architecture. The first phase involved surveying the database built in Stage 1 of the methodology for relevance to the chosen DRM enablers—SATCOM, TacSRT, and Space Control. In phase two, the research team then classified which laws, policies, and events as either enabling factors or constraining factors for the respective DRM enablers. In phase three, the research team investigated the constraining factors to determine whether constraints emerged from law or from policy, list the individual barriers posed from each legal and policy constraint, and categorize barriers as either operational or cultural in nature. Phase four entailed a thematic analysis of the individual barriers.

Interview Analysis: The team supplemented the first round of document analysis with an analysis of data collected through interviews. The research team generated an initial consolidated list of

observations and key takeaways from each interview conducted. Subsequently, the research team conducted a thematic analysis to identify patterns across both interviews. Interview themes were then matched with the barriers and themes identified from the first round of document analysis to produce consolidated barrier types.

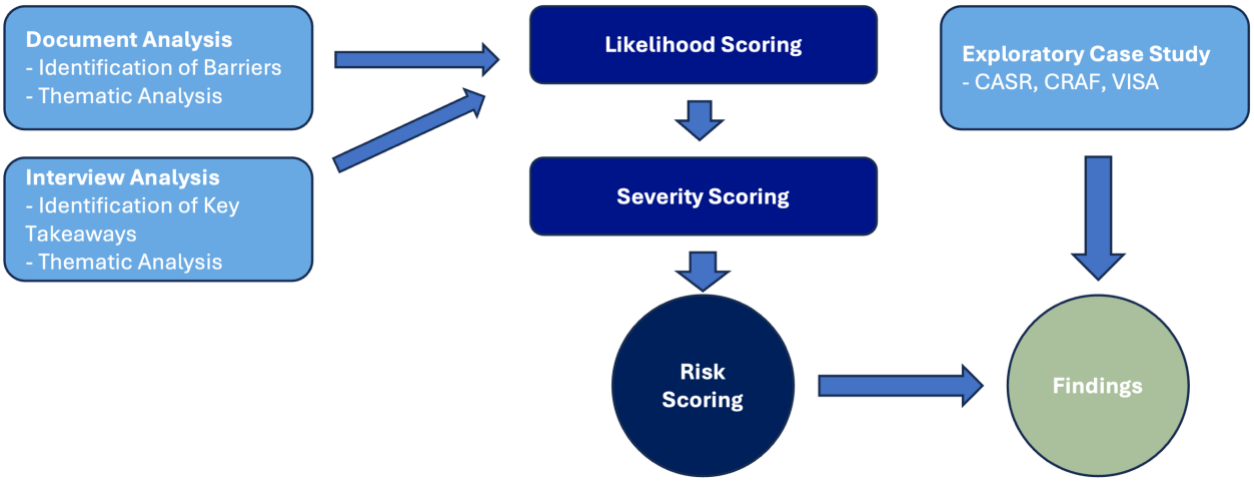

Figure 11. Execution of Multi-Method Approach to Risk Analysis

Likelihood and Severity Scoring: With the themes derived from document and analysis, the team proceeded to score each theme in terms of likelihood and severity.

Table 5 evaluates how likely barrier types are to occur based on asset ownership type: US-owned, commercially owned, or owned by allies and partners. The research team used a 5-point Likert scale to assess likelihood (1 = Extremely Unlikely, 2 = Unlikely, 3 = Neutral, 4 = Likely, 5 = Extremely Likely). A single number was chosen for each entry based on SME evaluation of preponderance of evidence and experience.

DRM	Type	Barrier Type	Likelihood Score		
			US	***Commercial***	***Allies & Partners***
SATCOM	*Operational*	Data fidelity	2	1	4
		Risk of outdated technologies threatening interoperability	4	2	4
		Unpredictable debris tracking capabilities and management	4	4	4
		Data and platform vetting requirements slowing mission speed	4	2	4
		Outdated technologies threatening mission capability	5	3	4
	Other	Licensing and regulatory requirements raising costs of cooperation	5	4	5
		Classification issues limiting information sharing	5	1	5
TacSRT	*Operational*	Proliferated environment increasing collision risks	4	3	3
		Proliferated environment increasing data fidelity risks, particularly from older assets	4	4	4
		Limitations on data sharing slowing missions in hybrid environments	4	2	4
		Loss of tactical custody and tasking latency increasing collision risks	4	3	3
		Limitations on data access and use creating barriers to commercial involvement	3	2	3
		Domestic controls on technology ownership and technology sharing increasing costs of cooperation	4	4	4
		Data access and validation issues limiting cooperative potential	3	2	3
	Other	Notification requirements slowing mission execution	4	2	5
Space Control	*Operational*	Lack of integration and interoperability mandates	5	4	5
		Dual-use technology restrictions impeding cooperation between US commercial and non-US	5	3	4
		Debris avoidance requirements reducing freedom of maneuver	4	3	4
		National decision authorities limiting/slowing execution of time-critical missions	2	1	4
	Other	Licensing and regulatory requirements limiting technology and information sharing	4	3	4
		Fidelity of commercial data creating liability issues and potential sources of insider threat	4	4	4
		Classification issues	4	4	4
		Transparent management of space assets can allow adversaries to gain critical knowledge of intent and capabilities	5	1	5
		Approval/notification dynamics limiting/slowing execution of time-critical missions	3	1	4

Table 5. Likelihood of Barriers by Type, DRM, and Asset Ownership

The research team also used a 5-point Likert scale to assess severity. (1 = No Impact, 2 = Minor Impact, 3 = Moderate Impact, 4 = Major Impact, 5 = Severe Impact). A single number was chosen for each entry based on SME evaluation of preponderance of evidence and experience (see Table 6).

DRM	Type	Barrier Type	Severity Score					
			US		Commercial		Allies & Partners	
			Mid-term: 18 mo. to 5 yrs.	Long-term: 5+ yrs.	Mid-term: 18 mo. to 5 yrs.	Long-term: 5+ yrs.	Mid-term: 18 mo. to 5 yrs.	Long-term: 5+ yrs.
SATCOM	*Operational*	Data fidelity*	4	5	3	5	4	5
		Risk of outdated technologies threaten interoperability	3	4	2	2	4	3
		Unpredictable debris tracking capabilities and management	4	3	1	1	3	2
		Data and platform vetting requirements slow mission speed	2	2	1	1	2	2
		Outdated technologies threaten mission capability	4	3	1	1	4	3
	Other	Licensing and regulatory requirements raise costs of cooperation	1	1	2	2	3	3
		Classification issues limit information sharing	3	3	1	1	3	3
TacSRT	*Operational*	Proliferated environment increases collision risks	2	3	3	2	2	2
		Proliferated environment increases data fidelity risks, particularly from older assets	2	2	1	1	2	2
		Limitations on data sharing slow missions in hybrid environments	2	2	1	1	2	2
		Loss of tactical custody and tasking latency increases collision risks	4	5	5	4	4	5
		Limitations on data access and use create barriers to commercial involvement	2	2	3	3	2	2
		Domestic controls on technology ownership and technology sharing increase costs of cooperation	4	4	2	2	4	4
		Data access and validation issues limit cooperative potential	2	2	2	2	2	2
	Other	Notification requirements slow mission execution	2	2	2	2	2	2
Space Control	*Operational*	Lack of integration and interoperability mandates	4	4	1	1	4	4
		Dual-use technology restrictions impede cooperation between US commercial and non-US	2	2	2	2	2	2
		Debris avoidance requirements reduce freedom of maneuver	4	4	1	1	4	4
		National decision authorities limit/slow execution of time-critical missions	4	4	1	1	4	4

	Other	Licensing and regulatory requirements limit technology and information sharing	3	3	2	2	3	3
		Fidelity of commercial data creates liability issues and potential sources of insider threat	4	4	4	4	4	4
		Classification issues	3	3	1	1	4	4
		Transparent management of space assets can allow adversaries to gain critical knowledge of intent and capabilities	4	4	4	4	4	4
		Approval/notification dynamics limit/slow execution of time-critical missions	4	4	2	1	4	4
*Includes cyber threats								

Table 6. Severity of Barriers by Type, DRM, and Asset Ownership

Risk Analysis. To assess risk levels, the team combined the likelihood and severity scores for each type of barrier to produce a risk-scoring matrix shown below in Figure 12. As a function of likelihood (1 to 5) and severity (1 to 5) scores, barriers are classified as either low risk (green cells), moderate risk (yellow cells), or high risk (red cells). The team assessed risk levels for both the mid-term and long-term time horizons across each type of asset ownership—US, commercial, and allies and partners.

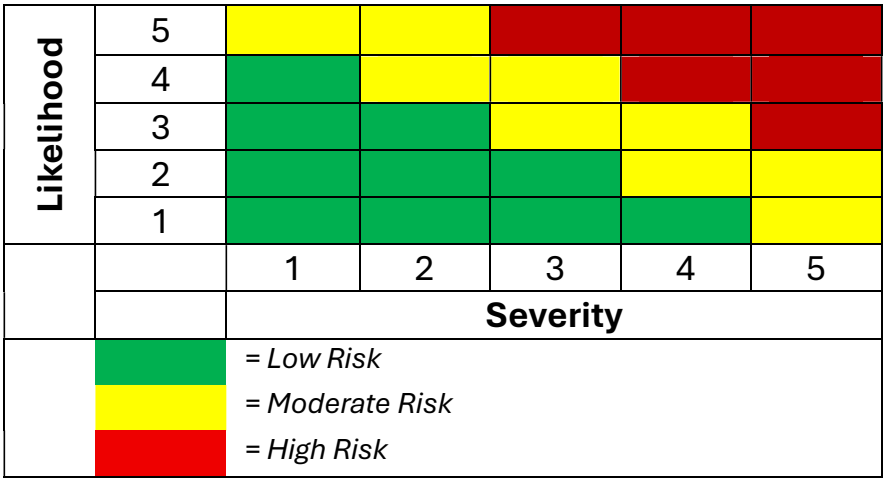

Figure 12. Risk-Scoring Matrix Based on Likelihood and Severity of Barriers

Exploratory Case Study: To explore how risks manifest in a hybrid architecture partnership, the team assessed how the USG currently incentivizes commercial and international partnerships through current policy and law and a preliminary examination of CASR. In particular, the exploratory case study examined issues related to asset protection, indemnification, and insurance.

Takeaways from the CASR case study and the risk analysis were integrated into study findings.

Stage 3: External Validation

In Stage 3, the findings from Stage 2 were externally validated by a dedicated Red Team and an independent Technical Advisory Team to produce conclusions and recommendations.

Red Team

The research team utilized a dedicated, external Red Team to validate the research approach, adjudicate research findings, and interrogate the feasibility of recommendations. The research team chose three external SMEs outside the Potomac Institute network to serve as the Red Team. The research team held three red teaming exercises during the period of performance.

Technical Advisory Team

In addition to the Red Team, the research team presented research and preliminary findings to a Technical Advisory Team composed of select members of the Potomac Institute Board of Regents, Senior Fellows, and network SMEs. The purpose of these sessions was to validate the research approach, provide feedback on research execution, and ensure the research findings met the Potomac Institute standards, including their utility for the client.

The research team chose four members for the Technical Advisory Team based on individuals with substantial space expertise across policy, legal, technical, commercial, and operational expertise categories. Technical advisors included:

- Mr. Eric Felt: Mr. Felt is an experienced, driven Space Technology Strategist with 20+ years of defense aerospace experience leading laboratory, test, program office, and Pentagon staff organizations;
- Mr. Brian J. Morra: Mr. Morra has over 40 years of experience in general management, strategic planning, and business development in the aerospace and defense industry;
- Dr. Robie Samanta Roy: Dr. Samanta Roy has over 30 years of aerospace, policy, defense, and industry experience;
- The Honorable Alan R. Shaffer: Mr. Shaffer has over 40 years of experience in defense acquisition and sustainment, research and engineering, NATO international affairs, and energy security.

The research team conducted eight review sessions with the Technical Advisory Team. Because these panel sessions were conducted using structured focus group interview methods, information from these sessions were attributed to meeting dates instead of specific individuals to accurately reflect the methodological distinction between individual interviews and focus group interview methods.

APPENDIX C: DEFINITIONS

To ensure clarity of communication and mitigate confusion regarding the use of terms and descriptions, a lexicon of key terms is included below. By clearly defining and limiting these terms, the research team hopes to avoid unintended lexical assumptions or recharacterizations.

Allies: Any country the United States has entered into a common defensive military alliance with (such as members of NATO, Australia, New Zealand, Japan, or the Republic of Korea), or that is designated as allied by the Secretary of Defense with the concurrence of the Secretary of State.[36]

Allied by Design: Allied by Design is the system or process by which US allies are incorporated into the development of integrated defense space systems and systems-of-systems from inception.

USSF Space Systems Command has declared that future government-owned systems should be "Allied by Design." This concept encourages the development of integrated defense space systems and systems-of-systems from inception. According to Space Systems Command, integrating allies' national assets into the space enterprise, co-developing capabilities, leveraging tools such as foreign military sales to bring space systems to new partners, and working with the global space industrial base achieves *"Allied by Design."* [37]

The research team assumed that Allied by Design is a goal and discussed avenues by which government integration is achievable, regardless of the country of origin of one or more system elements.

Blended ownership: A mix of US and commercial systems needed to fully accomplish mission objectives where outputs of sovereign and commercial systems are combined to yield actionable data or information.

For example, if USG-generated imagery is fused with commercial imagery to generate a product for strategic, operational, or tactical use, the resulting capability would be based on a *blended* system. Blended systems will contribute to the makeup of hybrid architectures, and as such, should be accounted for when analyzing the approach.

Commercial system:[38] Any capability, system, or product—including software, hardware, or algorithm—that is owned by a commercial company, either domestic or foreign; and whose employment within any architecture, *hybrid or otherwise,* is determined by the commercial owner.

Commercial systems are typically provided via contracts for specified services. These contracts typically also define the command and control of commercial sensors.

For purposes of this report, the team simplified the definition of a *commercial system* to focus on two core elements—ownership and decision-making. If any system is owned by a commercial entity that makes final decisions regarding employment, the system is commercial. Commercial systems

[36] United States Space Force. (2025b). *U.S. Space Force International Partnership Strategy: Strength Through Partnership*.

[37] United States Space Force Space Systems Command. (2021). International Affairs (SSC/IA): Strength Through Partnerships. https://www.spaceforce.mil/Portals/2/Documents/SAF_2025/USSF%20International%20Partnership%20Strategy.pdf.

[38] The study focused on this definition at the minimum viable capability level for ease of discussion.

may be developed and owned by US companies or by non-US companies. Where necessary for study completeness, the research team made this distinction.

This designation does not apply to systems whose components may be commercially procured but are integrated into a *government-owned* system.

Government-owned system: Any capability, system, or product—including software, hardware, or algorithm—that is owned and controlled by a government through acquisition and whose employment within any architecture, hybrid or otherwise, is determined by the government owner.

Government-owned systems may be operated by government personnel or contractor personnel hired by the government. This study made no distinction between the two in the definition of a government-owned system. If a government has procured a system and makes decisions as to its use, the research team declares that system to be government-owned.

Government-owned systems may be owned by the United States or owned by a *partner nation* (defined on the next page). Where necessary, the study made this distinction for completeness.

Hybrid Architecture: Hybrid architecture describes the integration of emergent "new space" commercial capabilities with traditional government-owned space systems.

The research team adopted the SmallSat Alliance definition of hybrid architecture, expanding it to underscore the critical importance of *interoperability* and the inclusion of allies and partners (see SmallSat Alliance Definition, below).

For our purposes, a hybrid architecture as described in the problem statement is composed of three major components: *a USG component* with elements from the DoD, IC, and civil agencies, *an international component* with elements from allies and foreign partners, and *a commercial component* with both domestic and foreign capabilities and services.

Hybrid architectures are also *interoperable*. They must be able to rapidly exchange data among satellite systems and services that are large and small, government and commercial, and US and allied across diverse and layered orbits.

The SmallSat Alliance Definition of Hybrid Architecture[39]

The SmallSat Alliance, established thought-leaders in hybrid architectures, define hybrid architecture as:

The concept of seamless integration between commercial and government-owned systems, regardless of their country of origin. Just as space is the ultimate global commons, the goal of a Hybrid Architecture is the "borderless" operation of government-owned and commercial space systems to the benefit of all in a fully participative manner.

In their 2020 Statement of Principles, the Alliance argue that hybrid architecture should leverage the following:

[39] SmallSat Alliance. (n.d.). *Hybrid Space Architecture Statement of Principles*. SmallSat Alliance. https://smallsatalliance.org/wp-content/uploads/2020/09/Hybrid-Architecture-Statement-of-Principles-v21.pdf.

- *Multi-path, adaptative, secure communications; open mission systems; and common standards*
- *Edge processing; autonomous command and control; AI/ML; and distributed ledgers (e.g., blockchain)*
- *Commercial space manufacturing efficiencies (e.g., additive manufacturing at scale), systems, and data; digital modeling, design, and engineering; standards for cyber protection and secure supply chains; and Agile/DevOps software and hardware approaches*
- *Low-cost commercial bulk launch; responsive and resilient small launch*
- *Rapid government acquisition mechanisms to move quickly to the new architecture*

Law: Legal authorities and obligations derived from the US Constitution, statutes passed by Congress, Senate-ratified treaties, and case law.

National Security Space Enterprise (NSSE): The people, organizations, systems, policies, and processes the United States uses to develop, acquire, operate, and protect space capabilities that support national security. At its core, the NSSE ensures that space-based capabilities support:

- Military operations
- Intelligence collection
- Strategic deterrence
- Homeland defense
- Allied and coalition operations

Partner nation: A partner nation is a nation with which the United States cooperates in a specific situation or operation.[40]

Policies: Policies are statements of intent that can include guidelines for decision-making and action and are generally not legally binding. Policies encompass Executive Branch strategies, doctrines, orders, directives, memoranda, instructions, department/agency regulations, and international agreements that do not require Senate ratification.

[40] (2025). In *DoD Dictionary of Military and Associated Terms*. Department of Defense.

www.potomacinstitute.org

901 N. Stuart Street
Suite 1200
Arlington, VA 22203
202.525.0770