TARGETS, TREATIES, AND TRADE SECRETS

Understanding Space Hybrid Architecture's LEGAL CHALLENGES

Kim Sloan, Todd Pennington

April 2026

In collaboration with
The Institute for National
Strategic Studies

901 N. Stuart Street, Suite 1200
Arlington, Virginia 22203
Phone: (703) 525-0770

www.potomacinstitute.org

KEY POINTS

- The legal challenges facing a United States Space Force (USSF) hybrid architecture raise old and new questions about incorporating commercial systems into operations. None are insurmountable, but solutions will require sustained effort.
- Each participant in a hybrid architecture will have their own motivations, risk calculations, and legal guidelines for participating. These must be taken into account by commanders who seek to effectively operationalize these tools.
- Adversaries may assume all participants in a hybrid architecture digital infrastructure are lawful targets. This may impede participation in such an architecture, especially if insurance and indemnity issues remain unresolved.
- The challenges facing a USSF hybrid architecture are similar to issues encountered in other domains, and lessons can be learned from these examples.
- Commanders will not be able to influence every aspect of a hybrid architecture; however, pre-planning and advance consideration can improve the system's effectiveness.

INTRODUCTION

Space is a domain accessible to all states for civil, commercial, military, and intelligence activities. The continuous and interactive relationships among these sectors, in a domain also accessible to allies, competitors, and adversaries, changes the character of modern conflict. The Department of Defense (DoD) can no longer rely exclusively on exquisite government-owned and -controlled systems to relay intelligence from the battlefield to decision-makers. Instead, the DoD strategy for joint warfighting includes a United States Space Force (USSF) hybrid architecture comprised of multilayered publicly- and privately-owned systems to enable the seamless flow of data during peace and conflict.[1]

A hybrid architecture includes technologies owned by governments (i.e., DoD and intelligence community), international participants (i.e., allied and foreign partners), and civilian elements (i.e., domestic and foreign commercial businesses).[2] Yet, when merged for use in conflict, the apparent distinctions among foreign, domestic, military, and civilian elements can become obscure.[3] The unified purpose and networked interconnection of such an architecture can make any participant a potential lawful target.

To effectively use a hybrid architecture in a conflict, commanders will need to understand the legal considerations, arrangements, guardrails, risks, and challenges of the individual participants, whether sovereign countries or commercial entities. Participants in any hybrid architecture are driven by their own interests to maximize mutual benefits and minimize risks.[4] While commanders can mitigate some hybrid architecture participant risks and employment challenges during conflict,

it is vital to negotiate and explore commercial and international capabilities, options, and restrictions prior to conflict. The peril of wartime commercial losses or foreign nations' legal restrictions may deter coordination and participation in a USSF hybrid architecture. Balancing political and financial risk considerations is not optional. They are calculations that international and commercial participants in a hybrid architecture must face. Navigating these realities and operating a flexible and effective hybrid architecture will require commanders to maintain a clear-eyed understanding of commercial and international interests and incentives.

Many of the challenges facing a USSF hybrid architecture are neither new nor revolutionary. The government has negotiated commercial and international arrangements for other domains in the past. The most successful (and costly) commercial augmentation for warfighting arrangements has involved mass global transport of troops and war materiel to and from theaters of war. A hybrid architecture for space warfighting will be more complex because the potential missions are continuous, more diverse, increasingly defined by intellectual property rather than massive physical equipment, and involve less mature legal structures.

This paper builds on the recent Potomac Institute for Policy Studies report "Making Space: Clearing the Way for Hybrid Architecture." Whereas that report created a framework to understand and evaluate policy and legal barriers, this supplemental work discusses potential legal considerations that could impact a commander's ability to use a space hybrid architecture in conflict. The intent is to increase awareness of how other participants may influence USSF hybrid architecture operations, and commanders' need to understand and manage those risks.

This paper proceeds in six sections. The first section elaborates on the importance of hybrid architectures for USSF in our current digital landscape. It then explores how the complexity of the landscape leads to dilemmas of coordination and differing risk calculations among military, government, and commercial participants. The third section identifies potential legal issues that participants in the space hybrid architecture may experience. To provide insight for resolving these issues, the paper draws lessons from eight examples where governments and companies partnered to achieve a military goal to examine risk and reward challenges. Fifth, the lessons were applied in a space-focused hybrid architecture to analyze commander options. Finally, the paper lays out key observations commanders should consider in the employment of a USSF hybrid architecture.

THE IMPORTANCE OF HYBRID ARCHITECTURES

Ensuring American space superiority is a continuous effort to help secure the nation's economic and security interests. Today, the commercial sector plays increasingly vital innovation and infrastructure roles in the space domain, including support for government operations. Space superiority is not fixed; it must always evolve to match the current moment and threat. For the fast-changing, globally arrayed space sector, that requires harnessing the flexibility and innovation of the commercial sector and the regional access, expertise, and relationships of allies and partners. An effective hybrid architecture maximizes the scale, capability, and flexibility of space support to the warfighter. Space Force leadership has argued that without an effective hybrid architecture, access to space can be compromised and the ability to operate freely in the domain is at risk.[5]

Hybrid architectures offer the USSF a way to leverage military, civil, and commercial space assets into an integrated and unified system. The goal of a hybrid architecture is the seamless operation of government-owned space systems with commercial and international systems in a fully

participative manner that benefits all involved.[6] For the USSF, the primary purpose is to achieve space superiority "to ensure freedom of movement in space for US Space forces while denying the same to our adversaries."[7] A hybrid architecture also provides numerous operational, tactical, and strategic benefits by enhancing the situational awareness, information advantage, and operational decision making of commanders directing forces.

Effective coordination of a hybrid architecture and its network interfaces is critical for space superiority. As defense strategies like the DoD Digital Modernization Strategy (2019), the United Kingdom's Digital Strategy for Defence (2021), and the Canadian Armed Forces Digital Campaign Plan (2022) make clear, society's digital transformation extends to its armed forces, greatly impacting US and allied military needs for, access to, and use of data networks.[8] The increasing prominence of commercial and international assets and infrastructure adds complexity to the design and operation of a USSF hybrid architecture. This is particularly true in wartime, when risk is highest and control over the digital battlefield is most crucial for space operations.

However, a USSF hybrid architecture creates new paradigms for international laws and borders. This also occurred when advancements in 20th century technologies and major wars evolved the world's awareness and understanding of national versus international waters and airspace. Wars can be exceptionally instructive in developing necessary international understandings, but they do not need to be the sole vehicle for testing. Understanding why, how, and when entities participate in a hybrid architecture provides important context if issues arise in how the USSF wants to use it.

THE DILEMMA OF COORDINATION

Our digitally networked way of life and warfighting increasingly relies on commercially developed hardware and software. In a hybrid architecture, this reliance will only increase. Private activity in the space economy far outweighs government activity in the areas of application and data. McKinsey estimated in 2024 that commercial space-enabled economic activity was approximately nine times government activity, or $270 billion for private commercial activities compared to $30 billion for government activities.[9]

The bottom line is that military power no longer rests only with government-owned assets episodically augmented by non-governmental capabilities.[10] Today, commercial and international assets play an ever more central role for contemporary military planning and warfighting as the joint force's data increasingly flows through platforms and networks not owned or controlled by the USSF. As a result of these changes, the military can no longer solely command and control a hybrid architecture, which creates a coordination dilemma. Doctrinally, command relationships among US forces are established by directive from a common superior. Command involving international forces is governed by treaties or international agreements. Commercial services do not have command relationships with supported commands; under the law of war, they are civilians "accompanying the armed forces."[11] The services they provide are a form of support to military operations (distinct from the command relationship of "support" to a peer command).[12] The scale and capacity of a hybrid architecture further complicate command relationships.

Thus, decisions by companies and foreign governments can and do directly impact the military's reliance on a hybrid architecture to fight and win in space.[13] The convergence of governmental, international, and commercial interests and capabilities inside a hybrid architecture can become more than the sum of its parts. It can also be a source of gaps and seams, to the extent that interests

diverge and the perception of the benefits associated with participation is diminished.[14] A commander's awareness of participants' own unique legal perspectives and considerations may help commanders understand why and when a participant may balk at supporting USSF actions.

PARTICIPANT LEGAL OBLIGATIONS.

Every participant in a hybrid architecture (governmental, commercial, or international) is governed by distinct legal obligations, which guide their decision making. Many of the issues that arise in a hybrid architecture are not new, but the technological challenges involved have new importance inside a space hybrid architecture. Not all risks in a hybrid architecture can be assumed and managed by commanders. Legal, policy, and contractual concerns can come into play for all participants. Understanding these issues and the perspective of the decision-makers involved can help overcome barriers and disputes.

Governmental

From the perspective of the US military, decision-makers planning to use commercial assets for military purposes are accustomed to considering the legal and policy guardrails that directly govern their behavior.[15] Beyond legal obligations and requirements, commanders also rely on military judgment both in the use of violence and restraint. This can include self-regulating conduct, to control escalation or avoid creating new norms favorable to an adversary.[16]

Governmental decision making is not monolithic; different agencies and branches will have competing interests, approaches, and methods for addressing problems. This is particularly important in a hybrid architecture where military assets may interact with non-military assets from NASA, the intelligence community, or other participants.

Commercial

Commercial services have long been used in support of military activities. Among the most comprehensive and enduring forms of commercial augmentation is the use of commercial shipping and commercial airlines for a singular purpose: transportation of personnel and equipment to or from a theater of crisis or conflict. These arrangements tap mature commercial markets in which transportation services have been essentially commoditized, and for which commercial augmentation arrangements have benefited from decades of commercial and military experience. The long-haul commercial transportation market is also one for which DoD can be both a steady-state market customer as well as a surge user during crisis or conflict.

The commercial space market is qualitatively different from the commercial long-haul transportation market in many ways. Commercial space is less mature and the differences in its peacetime and conflict usage are less clearly understood. Unlike transport services, hybrid architecture participants are often used to create enduring capabilities that keep information and services flowing smoothly. The nature of these enduring capability contributions, particularly as a form of redundancy, increases the likelihood that commercial and allied assets become legal targets at some point. Indeed, they have already been targeted as such.

Most significantly, for most companies, domestic laws impose a fiduciary duty on company directors and officers to exercise business judgment in the best interest of a company's owners or

shareholders. This means business judgments about risk, profitability, and the company's own legal compliance—*even for activities in support of national security objectives*—are driven, in part, by legal requirements prioritizing private interests. This can be a source of litigation and legal risk for commercial actors.[17]

To the extent possible, risks associated with inclusion of commercial capabilities in a hybrid architecture should be anticipated and addressed during pre-crisis integration. Constraints arising from either military risk or legal compliance considerations, or from commercial business judgment considerations, may take time to adjudicate. That time is available during pre-crisis integration but would become a stressor in an environment of crisis or conflict.

International

International participants in a hybrid architecture (including foreign companies and other governments) face their own legal dynamics distinct from those governing the US military. Foreign companies, like those in the United States, operate under fiduciary duty to act in the best interest of the company's owners.[18] As with US companies, business judgments about risk and profitability are based on a legal obligation to serve private interests. International commercial and governmental participants in a hybrid architecture owe primary allegiance to their own private interests or sovereign national interests and are subject to their country's domestic law. Generally, international participants in a hybrid architecture will have interests and legal frameworks closely aligned with those of the United States. However, this may not always be the case. Strategic interests, foreign domestic law, or differing legal interpretations of international law may all constrain international partners' roles in a hybrid architecture.

PARTICIPANT PERCEPTION OF RISKS.

Three distinct risk considerations (self-interest, interdependence, and negative externalities) complicate the coordination of governmental, commercial, and international participants in a hybrid architecture.

Risks to self-interest

Generally, risks to self-interest include impacts to the warfighting mission, disruption of profit potential, or loss of business or investment capital. Hybrid architectures inherently involve entities with differing and often competing interests and legal obligations. Governmental elements, whether US or foreign, will generally assess risk in terms of mission execution. For governments, self-interests are inherently political (or in the context of warfighting, military) and usually resource constrained. In contrast, commercial actors are (by definition) primarily motivated by the pursuit of profit.

Interdependence risks

Hybrid architecture elements must also account for interdependence risks. By design, actors in a hybrid architecture rely on and are affected by the capabilities and actions of each other. While the potential risks for a single participant may not directly impact others, the interdependent nature of a hybrid architecture means that others will be affected by and must account for how that single

participant assesses and responds to its respective risks. These interdependencies can produce suboptimal decisions and actions across the hybrid architecture. For example, governmental decision making must contend with the effects of commercial risk assessments. Similarly, commercial action can be enabled or constrained by insurance underwriters.

Risks of negative externalities

These encompass the ways in which hybrid architecture impacts entities and assets in the broader civil and commercial space sectors. For instance, a hybrid architecture relying on "Guardian Angel" satellites[19] might produce orbital debris that can affect actors outside the hybrid architecture. More broadly, hybrid architecture dynamics could create ripple effects that alter corporate markets, investment decisions, or adversarial targeting methods. Similarly, government reliance on legal tools to compel commercial entities to provide services can alter and potentially distort the very commercial qualities of the service that made them valuable.

Risks during conflict are uncertain and variable. No plan survives first contact with an enemy. Commanders and companies alike will evaluate their risks continuously, and partners that were once willing may become reluctant. Commercial insurance protections that were offered may be retracted. The exact dimensions of risk, as well as the risk calculations, legal guardrails, restrictions, or enablers, may not be known or knowable until conflict develops. While wargaming and pre-planning can reduce the likelihood of complications, unforeseen risks will arise.

When participants' risks outweigh their perceived gain, commanders may encounter problems using a hybrid architecture to complete missions. The following ten legal considerations frequently arise when commanders and legal experts discuss hybrid architecture and conflict. Many of these will likely shape a commander's ability to effectively manage a USSF hybrid architecture.

TEN LEGAL ISSUES

To stave off potential internal conflicts due to various participant concerns, it is crucial to understand the legal considerations in advance of any outbreak of fighting. The following section explores ten distinct legal issues where participants face differing legal obligations and different types of risk. This list is not exhaustive of all issues but highlights how understanding the interaction between laws and risk considerations is critical for a successful USSF hybrid architecture.

While the following issues may be planned for or mitigated in advance, the true test of these strategies and potentially the only solutions that can be identified may arise only during conflict.

ISSUE #1: THERE ARE LIMITS TO USING LAW BY ANALOGY TO MARITIME AND AVIATION DOMAINS IN SPACE.

Domain-specific principles of maritime and aviation law cannot be neatly applied by analogy to outer space. However, many problems of outer space law have never been tested in actual state practice.

The use and exploration of outer space is governed by the relatively mature and widely ratified Outer Space Treaty of 1967 and its implementing agreements.[20] Yet, despite this maturity, there is little state practice for many of its provisions. No states have sought recourse for damages through the

third-party liability adjudication procedures of the Liability Convention of 1972. The due regard consultation mechanism of Article IX of the Outer Space Treaty has never been invoked. Missions to the lunar surface have not yet reached levels of scale or persistence that brings the Outer Space Treaty's principles of free access and non-appropriation into tension.

The relative dearth of state practice in outer space, compared to more mature domains such as the high seas, may tempt one to reach for analogy to maritime or aviation law when the law of outer space is not clear in a particular context. Some scholars explicitly embrace this approach.[21] However, law by analogy always requires caution. Space, as a new domain of human activity in the 20th century, necessarily built on lessons and concepts originally developed on land, at sea, and in the air. However, the limits of experience in space exploration—and in particular, space warfighting—tend to constrain the usefulness of analogy to legal practice or precedent forged in other domains.[22] The law of naval warfare and the relatively newer law of air warfare are both imbued with hard-earned lessons forged by experience of war in those domains.[23] Such experience does not exist with respect to space.

The limits of law by analogy have two major implications for a hybrid architecture.

First, it means that a hybrid architecture may have to contend with domain-specific matters for which there is not always a fully agreed legal position. For example, this may arise in the context of questions about the extent of a country's "international responsibility" (under Outer Space Treaty Article VI) for commercial space services provided by companies from that country.

Second, when different interpretations are possible, some states may seek to apply legal principles of international responsibility from more mature domains such as the high seas.[24] Resolving such matters may entail coordination challenges within a hybrid architecture. However, such matters can also become important state practice, useful for developing outer space law in ways that improve legal clarity over time.[25]

ISSUE #2: IMPLICATIONS OF "INTERNATIONAL RESPONSIBILITY" FOR NATIONAL ACTIVITIES IN SPACE ARE NOT FULLY KNOWN.

Actions of commercial spacecraft may be legally attributable to their government, or to the United States as operator of a space hybrid architecture.

One of the Outer Space Treaty's principles sufficiently adjacent to air and sea to tempt law by analogy is the Article VI principle that states are "internationally responsible" for the activities of their nationals in space. This is true whether those activities are undertaken by the government or by non-government actors. Little state practice informs the full significance of this "international responsibility," but it is almost certainly something different from that of a flag state for ships, or a state of registration for aircraft.

Commercial space companies are, by this principle, linked to their national government in ways not well-informed by extensive international practice or precedent. Similarly, a state has some form of international responsibility for the activities of companies operating under its "authorization and continuing supervision" (a requirement of Article VI). This has implications for matters as consequential as the law of neutrality, or as mundane as terms and conditions for use of commercial space-based data relays.

A hybrid architecture enabling new kinds of activities in space provides the opportunity to further develop the law of "international responsibility" for national activities in outer space.

ISSUE #3: COMMERCIAL PROVIDERS DIRECTLY SUPPORTING MILITARY FUNCTIONS MAY BE TARGETED IN WAR.

Use of commercial assets to gain military advantage subjects those assets to risk of being targeted in the event of conflict.

Commercial space systems are, as a general rule, civilian objects not legally subject to attack in war. However, civilian objects can also be used by warring parties for military purposes. When a military uses civilian space systems to obtain a definite military advantage, those civilian systems can become lawful targets.[26] Commercial entities that supply services used for warfighting, such as mapping information in target development and prosecution, become lawful targets under normal rules of targeting.[27]

This risk is not limited to just those commercial assets participating in an operation. The actual use of some commercial systems for military purposes may increase the threat exposure of all commercial actors in conflict. Adversaries may lack the capability (or motivation) to effectively distinguish which commercial systems are actually used to gain military advantage. In this case, even commercial actors not directly involved with a hybrid architecture may find themselves at increased risk of being targeted. This potential negative externality is a strategic consideration in evaluating the overall costs and benefits of a hybrid architecture.

The fact that commercial space systems could become targets in war does not mean that they cannot or should not be used in a hybrid architecture. Companies have proven their willingness to accept business involving high levels of risk to support their nation's wars, especially when financial risk mitigation is available. Historical examples like the Merchant Marines, the Maritime Security Program (MSP), and the Civil Reserve Air Fleet (CRAF) show that, when called upon, the nation's economic sector is usually willing to augment the armed forces. Significant lessons can be learned from these historical examples, and several are outlined in the next section.

However, companies must accommodate business realities alongside the national security considerations of their country. Business owners and executives assess war risk to a company's assets, revenue potential, and other business interests. Consideration of these interests may involve a risk-adjusted price for commercial services. In some cases, sound business judgment may lead companies to decline government business altogether or offer services only if government-provided war-risk insurance is available.

At the highest levels of risk, no commercially viable arrangement may suffice. In such cases, the government may rely on laws such as the Defense Production Act. Some provisions of the Defense Production Act may compel companies to accept defense contracts.[28] Other provisions authorize the government to pay a premium for goods or services essential to the nation's needs, but that are unavailable at the amount, quality, or location needed to meet national needs.

The Defense Production Act is neither a plenary authority nor a permanent authority: its provisions are subject to limitations. For example, the Defense Production Act cannot be used to compel contracts of employment. Similarly, many of its provisions are subject to overall funding limitations. Further, most provisions of the Defense Production Act are enacted with sunset dates; although its

authorities are customarily renewed, the renewal process often results in revisions to the act.[29] The "commandeering" authorities of the Defense Production Act are subject to such limitations, in part, because of the potential to be used "in a manner potentially in tension with traditional free market principles."[30] Reliance on such "brute force" authorities may produce friction in commercial relationships, among commercial owners, workforces, investors, and the broader commercial space market.

ISSUE #4: DUAL-USE ASSETS MAY FACE WAR RISK REGARDLESS OF ACTUAL USE.

Many space assets are useful for both military and civilian purposes; this can put them at risk in space warfighting.

Closely related to, but distinct from, the military use of specific civilian commercial assets is the issue of so-called dual-use assets. Services such as Earth observation, communications, and space object tracking are capable of military or civilian use. Under the law of armed conflict, dual-use assets used for military purposes lose their protected status and may become a lawful object of attack.

Civilian persons and property are protected under the law of war. However, the protection of civilian persons and property is not absolute; this protection may be lost if a person participates in hostilities, or if the property is used in a way providing either side military advantage. Many civil and commercial assets are inherently dual-use. Bridges, power stations, aircraft, or vehicles have obvious civilian uses, but can also be put to military use. Most space capabilities may also be considered dual-use.

From a law of war perspective, there is no intermediate category of dual-use objects—either something is a military objective or it is not.[31] A dual-use object may become a military objective by virtue of its nature, purpose, use, or location. In some circumstances, a facility such as a bridge, power station, or airfield may become a lawful military objective to deny an enemy its use, even if no actual military use has yet occurred.[32] Dual-use commercial space systems are most likely to become military objectives (i.e., a lawful object of attack) by virtue of their actual use in a hybrid architecture.

This potential for dual-use space systems to become the object of attack in war presents a number of risks. For example, companies choose to participate in a hybrid architecture—or decline to—for reasons that may include perceived risk to their assets and revenue potential. Financial risk mitigation options (such as government-provided war-risk insurance) may incentivize participation, but the implications of a decision to not participate may mean that a particular company's capability is not readily available to a hybrid architecture. Incorporation of dual-use-capable space systems in a hybrid architecture may pose negative externality risks to the broader economy. If dual-use assets are attacked because they are used to support military users, civilian customers of commercial space services may be impacted by loss of service, with secondary economic impacts to their civil or commercial uses.

Despite business sensitivity to activities that put their capital at risk, the profit potential of providing commercial services to a hybrid architecture remains high. The availability of government funding and the technological limits of current commercial capability are pacing factors for a hybrid

architecture, more than lack of market incentives. At present, commercial reluctance about selling space services for military use is rare.[33]

The military incentives for integrating commercial capabilities into a hybrid architecture are substantial. However, there are legal implications to how these incentives are characterized. Relying on commercial space capabilities to enhance military capability is lawful. Doing so with the intention of complicating the adversary's ability to distinguish satellites used for military purposes from those engaged in purely civilian activities is not. [34] Such intentional obfuscation of military operations among civilian activities could violate the same law of war principles that prohibit the use of human shields.[35]

There may also be a relationship between how dual-use space systems are integrated into military activities and the risk calculations of commercial providers. Commercial providers might assess that a particular adversary is not likely to honor law of war distinctions among military and civilian targets, regardless of the feasibility of making such distinctions. Such an adversary might be perceived as treating all satellites associated with its enemy as targets because of their dual-use potential. In this environment, business risk might not correlate with the purchasing state's compliance with the law of war. This may raise the overall risk to the commercial space sector, but diminish the additive risk associated with providing services to defense customers.

ISSUE #5: UNDERSTANDING THE CONSIDERATIONS FOR PROVIDING PROTECTION AND DEFENSE OF NON-US GOVERNMENT ASSETS IS ESSENTIAL.

Military need may motivate the DoD to use military force to protect and defend commercial assets, but that authority is not normally granted to military forces as a standing matter.[36]

Providing for the protection and defense of international partner assets or commercial space assets in the hybrid architecture could affect incentives for participation. The DoD Commercial Space Integration Strategy anticipates that "the use of military force to protect and defend commercial assets could be directed."[37] Such authority is not without precedent; however, neither is it automatic.

The authority to extend self-defense protection to commercial or foreign persons or property is not normally granted to US military forces as a standing matter. Such authority is normally reserved to very senior levels of government and further delegated only in the context of a particular operation. [38] A hybrid architecture may anticipate providing "protect and defend" support to commercial or international contributors but may not be able to guarantee such support.

When available to US forces (and acceptable to international and/or commercial actors) this "protect and defend" authority could be an incentive to participate in the hybrid architecture. However, there may be contexts in which commercial or international partners may not wish to be seen as within the self-defense purview of the US Armed Forces.[39]

Collective self-defense always requires the defended state's consent, and international partners may have their own legal or geopolitical reasons for withholding such consent.[40] Commercial actors are probably less likely to decline "protect and defend" support within a hybrid architecture, but the possibility cannot be ruled out.

ISSUE #6: INSURANCE AND INDEMNITY CONCERNS WILL NEED GOVERNMENT AUTHORITY.

Private war-risk insurance may be prohibitively expensive or unavailable. Legislation authorizing government-provided insurance may be necessary to close the gap for hybrid architecture participants.

Absent specific authority for government-provided insurance, commercial space actors bear the risk of loss when supporting a hybrid architecture. Companies invest enormous sums in developing and launching commercial systems into orbit. Commercial space providers potentially expose these investments to war-related risks by supporting a hybrid architecture.

Commercial insurance for space systems is often prohibitively expensive. It is frequently unavailable at any price. When it can be obtained, it usually excludes war-risk coverage.[41] However, all commercial insurance is subject to cancellation if the underwriting assumptions change. For example, following the outbreak of war in Iran, many commercial shipping insurers cancelled their war-risk coverage for vessels in waters adjacent to areas of conflict.[42]

Federal appropriations law does not permit the government to provide insurance or indemnification, without express legal authority to do so.[43] The Federal Tort Claims Act is one such authority, but it only provides recourse for those damaged through the federal government's breach of some duty of care. Excluded from the act's coverage entirely are claims "arising out of" the combatant activities of US Armed Forces.[44] More robust financial protection in the form of government-provided insurance or indemnification requires specific legal authority. However, Congress has only approved such authority in very narrow circumstances.[45]

Government-provided war-risk insurance could incentivize hybrid architecture participation. Commercial providers account for the risks to their capital assets and the limits of financial risk mitigation options when deciding whether to offer services useful in target development, and in deciding the price for such support. Government-provided insurance and indemnification may shift commercial providers' risk calculations in favor of providing defense services. Such financial risk mitigation potentially adds to the total real cost of using commercial services but might also provide a threshold financial risk mitigation framework around which more robust commercial insurance options could emerge.

ISSUE #7: STATES AND COMPANIES WILL ACT TO PROTECT IMPORTANT INTELLECTUAL PROPERTY INTERESTS.

7a. For many commercial space companies, their intellectual property is their most valuable asset. Companies have strong incentives to protect their intellectual property interests, even within a hybrid architecture.

Intellectual property consists of intangible proprietary creations of the mind. Algorithms, written texts, inventions, designs, and engineering blueprints are all examples of intellectual property. Commercial actors protect their intellectual property either via formal registration of a patent or copyright, or (more commonly, when advanced technology is involved) by protecting it as a trade secret. The government enjoys broad, but not unlimited, rights with respect to technical data related to commercially obtained goods and services.[46]

The integration of multiple commercial actors in a hybrid architecture may pose challenges for companies that protect their intellectual property as trade secrets. Legal protection for trade secrets

requires its owners to use "reasonable protective measures" to prevent competitors from discovering their intellectual property.[47] Courts have also upheld the right of government contractors to enforce such trade secret protections with respect to other companies, even when the government may enjoy more permissive data rights for its own use.[48]

Commercial space providers employ both trade secret and patent strategies to protect their intellectual property. The use of trade secrets and other private corporate information may complicate integration of business rivals in a hybrid architecture. However, trade secret approaches also limit adversary exposure to hybrid architecture technology covered as intellectual property (since patent records are available publicly).[49]

7b. States and companies have an intellectual property-like interest in protecting their own national technological advantages, typically through export control laws.

States can create and generate their own intellectual property-like assets, which are designed to provide national advantages in trade and conflict. United States export control laws protect that perishable technological advantage. These laws often apply to space technology directly, or to dual-use technologies (with potential civilian or military, or intelligence uses).[50]

Other countries have similar laws. For example, Japan's export control laws generally prohibit "arms export" to "countries involved in or likely to be involved in international conflicts." Japan generally exempts the United States from this provision, given the importance of the United States to the defense of Japan.[51] However, many states do not exempt all treaty allies from their export control laws. For example, under French law, export of defense articles or services to the United States is allowed but is subject to a licensing process.[52]

The US government is not normally motivated to protect others' intellectual property rights, particularly when doing so adds time or complexity to a process. Tension exists between the DoD's mission interests and commercial providers' intellectual property interests.[53] The Government Accountability Office has identified challenges with the DoD's management of data rights in its commercial acquisitions.[54]

Similarly, export control laws and regulations were not generally promulgated or developed with something like a hybrid architecture in mind. Compliance with US and foreign export control laws could be a pacing factor for a hybrid architecture.

There is no simple way to find the optimal balance between seamless integration and arrangements that protect commercial and foreign intellectual property. However, accommodating commercial and national interests in intellectual property and data rights can incentivize USSF hybrid architecture participation.

ISSUE #8: A HYBRID ARCHITECTURE SHOULD ANTICIPATE OPERATING THROUGH COMMERCIAL DISPUTE RESOLUTION.

Commercial dispute resolution processes will, from time to time, be necessary and may be beneficial in the long run.

A hybrid architecture must balance unity of effort with the organizational independence of its component parts. A hybrid architecture seeks technical and operational integration to achieve unity of effort. However, governmental, international, and commercial actors each have motivations to

preserve a degree of arms-length independence from other actors in a hybrid architecture. As the number and interdependency of hybrid architecture participants increases, the probability of legal disputes may also increase. Commercial actors in all cases, and international contributors to some extent, will participate in a hybrid architecture subject to their own obligations to maintain a degree of arms-length independence necessary to advocate their interests in the event of such disputes.

Disputes between and among commercial companies and their customers are neither unprecedented nor untested. There is a robust body of law, with extensive practice and precedent, regarding disputes with and among contractors that would apply to commercial participants in a hybrid architecture.[55] Hybrid architecture leaders should anticipate that operating through commercial dispute resolution processes will, from time to time, be necessary and may even be beneficial in the long run.

For example, prior to becoming a preferred launch provider, SpaceX had been unable to compete for National Security Space Launch contracts (at the time, awarded under sole source acquisitions). The Air Force only allowed SpaceX to compete for launch contracts after the company filed a lawsuit against the service.[56] Today, SpaceX is poised to provide the majority of Space Force launch missions. Thus, a legal dispute that was most unwelcome in 2014[57] ultimately resulted in improved Space Force access to space.

ISSUE #9: FOREIGN LAWS, POLICIES, AND INTERESTS WILL IMPACT INTERNATIONAL PARTICIPATION IN A HYBRID ARCHITECTURE.

International partners participating in a hybrid architecture will be bound by their government's domestic law, interpretation of international law, and sovereign policy regarding military activities, which may differ from that of the United States.

Whether acknowledged or not, international partners in a hybrid architecture hold veto power over how their space systems are employed. As sovereign actors in the international system, each state pursues its own national interest and applies both its own national laws and its own interpretation of international law.[58]

To ensure legal compliance, as the state understands it, each state can apply national caveats for the participation of its forces and its regulated commercial space actors when involved in hybrid architecture activities.[59] The rationale for such national caveats might not be fully explained or declared in advance. Historically, some have emerged only during combined operations.[60]

Similar considerations may arise if a hybrid architecture involves non-US private companies. These foreign-owned companies may be bound by their country's interpretation of law. They might also independently apply a different—and more restrictive—interpretation of what the law allows or requires.

Processes that accommodate national caveats may incentivize international participation. However, the proliferation of caveats (especially undeclared caveats) can and should be discouraged. The NATO Parliamentary Assembly has urged member states to minimize declared caveats and eliminate undeclared caveats so that restrictions on national participation may be considered during the planning process.[61] Incorporating similar ideals into the design of a hybrid architecture would be prudent. However, providing business rules and predictable processes for the

exercise of red cards during war games may lower the perceived political costs for international partners to integrate within a hybrid architecture.

ISSUE #10: STATE VIEWS DIFFER ON NON-KINETIC ATTACKS AS USE OF FORCE.

Each country will independently assess whether it views an attack as rising to the level of a formal "use of force" or "armed attack" under international law and will act according to its understanding of its national interests.

Under international law, "use of force" is derived from Article 2(4) the United Nations Charter. It states: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

The precise definition of "use of force" in this context has been a matter of some debate. Traditionally, it has referred to kinetic military actions—i.e., physical violence or armed attacks. In 1986 the International Court of Justice distinguished between the most serious forms of the use of force (those constituting an "armed attack") and other less grave forms. However, with new forms of non-kinetic attacks, such as cyberattacks, the interpretation of "use of force" is still evolving.

In kinetic operations, establishing the fact of an attack and attribution is normally straightforward. However, countries differ in their interpretations of when cyber operations and electronic warfare activities rise to the level of a "use of force" or "armed attack."[62] While some cyberattacks clearly fall below the threshold of "use of force," there is little consensus on what actions short of an armed attack do rise to that level.

Federal information technology systems and critical infrastructure are constantly under threat with over 30,000 information security incidents reported in FY2022.[63] These incidents are not treated as an "armed attack" because the damage is not widespread and sustained. In such cases, implementing cybersecurity protections is an appropriate and measured response.

The question about when a non-kinetic attack rises to the level of an "armed attack" remains unresolved even among experts in international law. [64] While consensus has proven elusive, the fact that cyber warfare and electronic warfare activities occur will force states to make decisions involving this unsettled area of law.

Whether an event qualifies as a "use of force" or an "armed attack" can have significance under international law and may also be relevant under a country's domestic law, both for the legal availability of proposed actions, and for characterizing adversary actions. For example, the government of Japan historically interpreted its constitution to permit the "use of force" (its term of offensive military action) only in the event of an "armed attack" on Japan.[65] Diverging approaches to legal interpretation are common in combined operations across domains. The United States and many of its allies and partners have experience addressing these matters in the context of countering terrorist networks and conducting cyber operations.[66] Such divergence is especially likely to arise in a space hybrid architecture, given the importance of cyber operations and electronic warfare to space missions.

Non-kinetic activities may be conducted as an integrated aspect of a larger "armed attack," as with the 2022 Russian cyberattack on Viasat, a US commercial company, which disrupted

communication services to the Ukrainian military ahead of the Russian invasion of Ukraine.[67] The event also impacted internet users across Europe.

***

The ten issues identified above can pose serious challenges to the smooth and effective operation of a hybrid architecture. The issues also offer insight into how differing legal obligations may be overcome with appropriate, early preparation and planning to posture the USSF hybrid architecture for operational success. While the space domain is not always analogous to the maritime and aviation arenas (as Issue #1 demonstrated) the other domains offer lessons learned about potential solutions that have proven useful in other domains. The next section provides context on ways some hybrid architecture participants have worked together historically and lessons drawn from those experiences.

HISTORICAL LESSONS LEARNED

The legal and policy challenges accompanying modern technological advances are daunting but, as history shows, not insurmountable. Successful wartime integration of commercial companies and international partners was possible in the past. Historically, the key to success was aligning financial incentives with thoughtful balancing of resilience and dependence. International integration requires balancing mutual security gains with latitude for sovereign prerogatives. Below are examples of US Armed Forces reliance on commercial or international structures with qualities similar to a hybrid architecture, and lessons that can be learned from each.

LESSON #1: GOVERNMENT INCENTIVES CAN ENCOURAGE VOLUNTARY PARTICIPATION.

When the need for global transportation has exceeded the organic capacity of the armed forces, the strategic imperative for global reach has driven policy changes. The experience of World War I demonstrated the need for military commanders to have alternative sealift options in case of future conflicts abroad. To address this need, Congress enacted the Merchant Marine Act of 1936. This act granted subsidies to owners of American-flagged commercial ships willing to guarantee their availability to offer commercial sealift capacity for national defense when required.[68] It also laid the groundwork for the creation of a commercial shipbuilding program and a federal training school for merchant seamen. This program effectively made the business benefits outweigh the substantial operational risks for companies to voluntarily participate. Ultimately, the value of a Merchant Marine was proven at sea during World War II, when it became the lifeline for the war-sustaining Lend-Lease Act.[69]

After World War II, the US government continued to provide legal authority to augment military sealift and airlift capabilities with commercial support. The legacy of the Merchant Marine endured under the Maritime Support Program, authorized under the Defense Production Act of 1950[70] and Maritime Security Act of 2003.[71] Similarly, the Civil Reserve Air Fleet (CRAF) program, also established under the 1950 Defense Production Act,[72] offers military commanders airlift support options during contingencies such as Operations Desert Shield/Storm and Operation Iraqi Freedom.[73]

To incentivize commercial participation in these programs, the government offers companies priority access to DoD cargoes and passenger fares in peacetime.[74] In return, participating transportation companies commit to making their commercial fleets and civilian crews available for use to transport armed forces personnel and cargo in times of crisis. For example, Delta Air Lines currently has multiple million-dollar, multi-year Indefinite Delivery Contracts for domestic charter airlift services in exchange for program participation.[75]

LESSON #2: GOVERNMENT-PROVIDED WAR-RISK INSURANCE REQUIRES STATUTORY AUTHORITY.

During war service, commercial vessels and crew are at risk. For example, in WWII, 733 Merchant Marine ships were sunk by enemy action; a greater percentage of Merchant Mariners died in the war than in any of the US military branches.

The commercial insurance market can seldom underwrite risk of loss for capital assets introduced into a wartime environment in which they are likely to be targeted by an enemy. The probability and scale of wartime losses typically exceed commercially viable coverage. Thus, Congress has enacted laws that authorize the government to provide war-risk insurance to companies participating in the Maritime Security Program (MSP) and the Civil Reserve Air Fleet (CRAF).

The Federal Aviation Administration (FAA) program offers hull and liability aviation insurance to CRAF participants during activations.[76] Government-provided aviation war-risk insurance is benchmarked on market costs prior to September 11, 2001, after which most insurance providers withdrew war-risk coverage from their aviation policies. The government also provides insurance for commercial shipping augmentation of defense forces through the Maritime Administration (within the Department of Transportation). Such government-provided war-risk insurance has been a structural hallmark of both MSP and CRAF. Similar authority will likely be important for a space hybrid architecture.

LESSON #3: COMMERCIAL SERVICES CAN CLOUD LEGAL STATUS IN CONFLICT.

When used for military purposes, otherwise civilian objects can become lawful targets in conflict. Merchant Marine vessels acting as auxiliary naval forces are normally treated as warships subject to attack during conflict.[77] Similarly, CRAF aircraft delivering troops to a war zone may lose their otherwise protected status during conflict.[78] In these legacy examples of commercial augmentation, the transition from civilian usage to military usage is clear and observable. For a space hybrid architecture, that may not be the case. Satellites performing commercial, civilian services one day could be providing defense services to warfighters engaged in conflict the next. The transition from civilian use to military use may not be observable and may not be absolute: many space systems could provide both military support and commercial civilian services simultaneously.

During 2025's Twelve-Day War, Iran targeted a Microsoft data center in Be'er Sheva. The Islamic Revolutionary Guard Corps, which was responsible for the attack, stated that Microsoft's close collaboration with the US DoD made it a lawful target.[79] They stated that it was a part of the system supporting aggression. During the 2026 conflict, Amazon Web Services data centers, and commercial infrastructure in the region were also attacked.[80]

Clarity of status might be possible if those satellites used for military purposes were declared or identified in space object catalogs. The legal clarity such declaration would provide would come at a cost (namely, simplifying an adversary's task of countering them). However, failure to do so could leave even uninvolved satellites vulnerable to targeting during conflict. Space systems used in warfighting do not lend themselves to the handful of special protections under the law of war, such as those afforded to medical transports and religious personnel.[81] In short, most components of a hybrid architecture designed for use in warfighting are likely targetable under the law of war in the event of hostilities, and even uninvolved satellites may share in wartime peril.

LESSON #4: TRULY COMMERCIAL SERVICES REQUIRE WILLING PARTNERS; GOVERNMENT EFFORTS TO COMPEL ACCESS TO ADVANCED TECHNOLOGY ARE LIKELY TO INVOLVE LEGAL DISPUTES AND LITIGATION.

The US government has strategies and guidance urging swift transformation for digital infrastructure, but law and policy to guide implementation is still developing.[82] The DoD's contract with Google is a prime example of how technological advances can raise new challenges in law, policy, and business judgment.

For example, in 2017 Google was quietly a subcontractor for DoD's Project Maven, which used artificial intelligence to analyze drone footage.[83] The software program successfully decreased analyst workload by approximately 60%, processing over 39 million gigabytes of full-motion video and enhancing military missions.[84] The project was an example of the military's digital transformation. However, in June 2018 Google workers became aware of the project due to leaked reports. Google employees expressed displeasure to management that the programming was being used to increase the lethality of offensive strikes, counter to many employees' values.

Caught between a lucrative business opportunity and workforce objections strong enough to imperil its retention of key employees valuable across other lines of business, Google opted to end its participation in Project Maven (even as it continued to support the DoD on other efforts like detecting corrosion on Navy ships).[85] Project Maven highlights the growing influence of Big Tech platforms in the military domain, and the role of values-informed business judgments within Big Tech companies.[86]

LESSON #5: EMINENT DOMAIN AND CONSCRIPTION MAY NOT ALWAYS PROVIDE THE DESIRED OPTION.

During World War II, the government often contracted commercial shippers for sealift services. However, sometimes the government requisitioned ships for war service via condemnation (i.e., it seized private ships and made payment of "just compensation" to owners), under the Constitutional principle of eminent domain.[87] The government usually contracted with shipping companies to crew and operate ships obtained this way. In either case, the government shared some or all of the financial burden for wartime losses with commercial shippers.[88] Both the burden and valuation of losses were commonly litigated in the event of wartime damage or loss of a vessel.[89]

Just as with the option to draft civilian soldiers, today's government retains, through the Defense Production Act, the power to compel operations, and seize control of companies or assets through coercive means. However, these coercive means may not facilitate the desired result.

In 2026, Anthropic sought to bind the uses for which its Claude AI tool may be used by the DoD. Anthropic reportedly wanted its terms of service for military use of Claude to restrict certain end uses. Anthropic's stated reason was "to ensure its tools aren't used to spy on Americans *en masse*, or to develop weapons that fire with no human involvement."[90] The Pentagon wanted Anthropic to be available for "all lawful purposes," and took punitive action against Anthropic to impose business costs for the company's position.[91] However, Anthropic's public response to the Pentagon's request has also generated interest and support for the company, without providing the desired benefit for the DoD.

The dispute, now in litigation, highlights challenges that can arise when a business decides—for whatever reason—to curtail its business relationship with the government.[92]

LESSON #6: ACCOMMODATING SOVEREIGN PREROGATIVES INCENTIVIZES PARTICIPATION.

The sovereign prerogatives of other countries are always a consideration in combined activities with US armed forces. This is true whether those prerogatives are explicitly acknowledged, or not. Using national caveats, international forces can be restricted from engaging in certain types of operations as a requirement of participation. Such caveats might arise from differing views of law, differing risk tolerance, or differing strategic interests. Whatever their motivation, such caveats are a complicating factor in achieving unity of effort.

For example, during NATO operations in Afghanistan, a detailed set of policies and processes emerged by which force contributing nations implemented their national caveats.[93] In other cases, allies have denied the United State use of bases or airspace for particular operations, even as cooperation continued in other matters. For example, several European countries did not allow US bombers launched from the United Kingdom to transit their airspace during a 1986 attack on targets in Libya.[94]

National caveats can be stated or unstated, worked out ahead of time or declared in the moment. However, without a mechanism to address national caveats (or other expressions of sovereign prerogative) during mission planning, they are likely to remain unknown and undeclared. They will instead emerge during crisis or conflict, when their impact on a unified hybrid architecture's operations is greatest.[95] A hybrid space architecture should not encourage or endorse national caveats, but should anticipate that processes to account for them may be necessary and useful for incentivizing participation.

LESSON #7: INCLUDING COMMERCIAL TECHNOLOGIES IN DIGITAL TRANSFORMATION BUILDS RESILIENCY.

The 2022 Russian full-scale invasion of Ukraine produced an example of how digital transformation enhances resiliency. During the invasion, the Ministry for Digital Transformation in Ukraine prioritized transitioning the government to a digital platform, including moving critical infrastructure and communications to internet nodes outside Ukraine via SpaceX's Starlink internet-access satellites, with government data stored and processed via cloud services from Amazon, Google, and Microsoft.[96] Although Russia targeted critical terrestrial infrastructure with traditional kinetic and non-kinetic attacks (i.e., missiles and cyber), Ukraine's access to space-based broadband ensured its citizens continued to receive government-provided services. From a tactical standpoint, Starlink's role in this digital transformation enabled real-time data network connectivity for Ukraine,

providing a resilient capability for command and control and allowing tanks and artillery to target Russian forces using commercially available unmanned aerial vehicle systems.[97]

LESSON #8: OVERRELIANCE ON COMMERCIAL SERVICES CAN BECOME A VULNERABILITY.

While commercial technology can provide resiliency, it can also produce dependency. Overreliance on commercial technologies can adversely affect operations. This can be especially risky in places where the commercial operator has monopoly or near-monopoly control over a capability.

For example, while Starlink provided Ukraine with communications resiliency, its reliance on Starlink has not always been an unqualified good. At one point in the conflict, Elon Musk restricted Ukraine's access to Starlink to prevent the system's use in a particular operation he did not want his company to support.[98]

Well-structured contracts minimize the risk of later disputes. However, no contract can perfectly account for all eventualities. Expansively scoped contracts may be more adaptable to unforeseen circumstances. However, when one party to a contract seeks an expansive scope, the other party tends to value residual control rights.[99] For a hybrid architecture, this tension between perfect adaptability and perfect enforceability of commercial contracts drives a negotiated balance of interests between the parties. Narrowly scoped contracts are less agile but tend to have more readily available remedies for failure to perform. Broadly scoped contracts are more agile but are also more likely to include residual control provisions for commercial providers.

***

Each of these eight lessons learned provides examples of governments and companies weighing costs, risks, and expected benefits. The Google/Project Maven and Russia-Ukraine War/Starlink examples highlight how military users of commercial services become, to some extent, dependent on the business judgments of commercial providers. Business leaders' law-imposed fiduciary duty to owners and shareholders may result in gaps between a company's interests and military needs. On the other hand, commercial or international capability may be so good that it invites problematic dependence.

APPLYING THE HISTORICAL LESSONS TO A USSF HYBRID ARCHITECTURE

As shown above, agreements between commercial entities and the DoD are not new. The MSP and CRAF are enduring structures for commercial augmentation of the US Armed Forces. However, a space hybrid architecture is likely to differ in many important ways. It is likely to encompass many missions rather than one. In this variety of missions, each may entail different technical, financial, and risk considerations. Furthermore, the MSP and CRAF were built upon capabilities already proven in commerce and in war; a space hybrid architecture is likely to involve many novel technologies with unproven commercial market potential. The United States has experience operating as part of a coalition and integrating commercial capabilities. However, commercial and international contributions to a hybrid architecture each bring unique value, and distinct legal and policy challenges.

Numerous legal issues are identified in this paper**, yet they are not insurmountable.** All can be overcome, but few can be legislated away by one-time rule changes, and commanders may not be

able to resolve them alone. There are three engagement levels: international, national, and DoD-business. Of these, commanders can influence two—national and DoD-business.

International engagement

Some of the legal issues (i.e., Issues #1, #2, #3, #4, #7b) are enduring challenges that predate the creation of a space hybrid architecture and will endure for the foreseeable future. These issues cannot be altered by US law or policy. These issues are based on international treaties and laws that a commander will likely not be able to directly modify. Lessons #3 and #4 highlight how commercial space providers can become targets in conflict, either through their actual use in support of military operations or due to the potential military value of dual-use capabilities. These considerations arise from principles of international law that cannot be changed quickly or unilaterally. Lessons #6 and #7 show how accommodating international prerogatives can boost participation. Of note, some legal issues relevant to a hybrid architecture are descriptive of law of war considerations.

The perception of allies also influences operations. Allies will interpret laws and agreements through their own unique legal perspectives (i.e., Issues #9 and #10). Engagement on these issues builds understanding, anticipates problems, and prepares commanders for complex operations. As previously noted, Lesson #6 shows that accommodating allied perspectives can strengthen alliances and improve operational flexibility.

National engagement

Some issues can be shaped by the USSF advocating for changes through policy or legislation (i.e., Issues #6, #7a, #7b, #8). Lessons #1 and #2 show how government-provided financial and risk-mitigating incentives (like those in MSP and CRAF) have been effective at incentivizing companies to support military efforts voluntarily, even when operational risk is high. However, Lessons #4 and #5 highlight that compulsion or coercion in acquiring services can erode reliability, incentives, and overall strategic value. Issue #6 (regarding war-risk insurance or indemnification) for a space hybrid architecture will probably require new legislation.

DoD-business engagement

While Issues #6, and #8 may involve national engagement, commanders can often address them through the chain of command and preplanning. Issue #5 (authority for protection and defense of non-US government assets) is not a standing authority; securing this authority in the context of a particular operation—or for the hybrid architecture on an enduring basis—will probably require detailed planning for each type of protect and defend activity contemplated.

Additionally, as seen in Lesson #8, overreliance on commercial services can become a vulnerability for commanders if they do not have alternative options. Commercial tech companies' business decisions may curtail DoD support. SpaceX, Google, and Anthropic have each, at times, made business judgment decisions to limit the scope of services offered to military users. Even where law provides the government options to overcome such business decisions, commercial actors normally have recourse to the courts and litigation. The resulting legal challenges add complexity and uncertainty to a hybrid architecture.

Anticipating these issues, building expertise to navigate them, and ensuring resilient approaches to operate through them will posture hybrid architecture warfighters for success.

KEY OBSERVATIONS

Observation 1: Few complex operational concepts have sufficient political support to secure broad exemption from the force and effect of other laws; hybrid architecture will be no different. A space hybrid architecture should anticipate overcoming problems on a case-by-case basis, rather than through a single, grand legislative reform.

> Hybrid architectures provide command flexibility, resilience, and targeting options, but come at the price of greater uncertainty in command structures. The priority should not be finding universal solutions to address all outcomes.
>
> Commanders should instead focus on adapting to and interacting with elements of the hybrid architecture as individual partners, rather than as military subordinates. International and commercial partners' contributions to a hybrid architecture will be governed by the applicable contracts or agreements. These may make valuable resources available to commanders but may also include restrictions or reservations that might not apply to a commander's organically assigned military forces.

Observation 2: Rather than a single common charter, arrangements for a space warfighting hybrid architecture may resemble a triad of bilateral arrangements. Government-commercial arrangements form one line of effort; government-international arrangements form another; commercial-international may form a third.

> Hybrid architecture participation will be governed by contracts and international agreements. The nature of these agreements with commercial and international partners differs. The actual instruments that bring in organizations and capabilities will be listed in contracts and international agreements, each constructed under its own body of law. Additionally, commercial space services, even for national security missions, must secure and adhere to the terms of operating licenses from agencies external to DoD (i.e., the FAA, Department of Commerce, and Federal Communications Commission).

Observation 3: A space hybrid architecture should be adaptable to various forms of command relationships. Historically, US forces have organized for war in several different ways. A hybrid architecture needs the flexibility to adapt to any of them, including simultaneous support of differently organized warfighting commands in different theaters.

> Command of a hybrid architecture will require a sophisticated leadership approach. Commanders will probably have directive authority over assigned US military forces. Their authority regarding international forces will depend on the force-providing agreements. Authority regarding commercial services depends on the contract.
>
> These dynamics suggest a complex leadership environment, but US Armed Forces have extensive experience with such arrangements. In the defense of Korea, three separate commands exist in parallel, with both distinct and overlapping responsibilities. The war in Afghanistan involved a multinational force leveraging NATO command processes. In the

defense of Japan, US and Japanese forces operate together in parallel, separate chains of command.

Similarly, the US Armed Forces are accustomed to operating with closely aligned contracted and commercial support. In the conduct of operations, there is no practical difference between "defense contractors" and "commercial services." Any distinction between the two may have relevance in thinking about how capabilities and services are obtained; it has no legal significance for how commercially obtained capabilities and services are employed. As with traditional defense contracts, the contracting officer concerned is ordinarily in the chain of command for addressing any issues regarding commercial services if a company's business risk calculations change during conflict in ways that can impact or alter a commander's access to services.

Observation 4: If structuring overall risk insurance for hybrid architecture participation becomes too difficult, rather than trying to make a one-size-fits-all formula, commanders may be able to structure such agreements based on individual mission risk.

When structuring financial incentives and war-risk insurance options, no single framework may be ideal for each commercial space mission represented in a hybrid architecture. Space missions such as space domain awareness and on-orbit refueling differ in many significant ways; such missions may require financial incentives and war-risk insurance options as different from each other in their particulars as MSP is from CRAF.

Observation 5: Securing authorization for military forces to protect and defend commercial or international space systems will probably require Concepts of Operations and Concepts of Employment that allow decision-makers to understand what they are being asked to approve. Concepts for protection and defense with great variance in technical detail or risk profile may benefit from distinct Supplemental Rules of Engagement provisions for each concept.

Protect and defend is a category of mission activities that could take many forms in the space domain. Authority to protect and defend commercial or international capabilities in a hybrid architecture may be contingent on a capability-specific concept of operations, which may require approval at echelons above the hybrid architecture. Thus, it is vital that commanders, military leaders, and hybrid architecture participants have a full understanding of the actual limitations and restrictions involved in any protect and defend arrangements.

Moving forward, early engagement with allies and commercial partners in wargaming and other efforts should identify friction points prior to conflict. Commanders can then resolve or elevate for legislative or policy solutions if possible. Future studies may be able to provide a more detailed map of legal issues, legislative recommendations, and potential courses of action commanders may take in specific scenarios to aid decision making.

CONCLUSION

The laws and policies guiding space are still developing, and the USSF has an opportunity to shape them in appropriate ways. Space-based systems have proven vital to every modern military operation, from Operation Desert Storm (1990) to Operation Epic Fury (2026). Coordinating data access and movement to and from space will be critical to the smooth and effective operation of the hybrid architecture that the USSF and DoD have proposed. Therefore, it is critical to establish

processes that anticipate and address a wide range of domestic and international legal and policy considerations prior to conflict. Most of the law and policy relevant to a hybrid architecture was enacted with a different or broader purpose in mind.

The issues facing a USSF hybrid architecture are complex but manageable. Disputes among participants in a hybrid architecture are to be expected. These disputes may even be necessary to strengthen and clarify domestic and international law in the simultaneously mature and emerging legal domain of outer space.

A space warfighting hybrid architecture will require the Space Force to broaden and deepen its organizational expertise in navigating the implications of administrative, commercial, international, and foreign law. It will require Guardians as sophisticated in business as they are in astrodynamics. It will require leaders unafraid of the inherently transactional quality of commercial deals. It will require international negotiators bold in advancing national interests but sufficiently creative to find win-win pathways for international partners. It will require a hybrid way of thinking before it can succeed in a hybrid way of fighting.

ABOUT THE AUTHORS

Kimberly Sloan, PhD is the Director of Research Strategy and Development at the Potomac Institute for Policy Studies. Her research expertise focuses on intelligence, defense, concept development, and wargaming.

Todd Pennington, Esq is Senior Fellow for Space Strategy and Policy at National Defense University's Institute for National Strategic Studies. He is also affiliated with Georgetown University Law Center as Adjunct Professor of Law, and as Senior Fellow at the Center on National Security. He is admitted to practice law in the District of Columbia, Virginia, and Tennessee. He previously served as Assistant Deputy General Counsel for Intelligence (with portfolio for space operations) for the DoD, and as Senior Assigned Legal Counsel for United States Space Command and the United States Space Force.

ENDNOTES

[1] 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).

[2] For purposes of this and the *Making Space: Clearing the Way for Hybrid Architecture* report, hybrid architectures are network integrated, interoperable, must be able to rapidly connect, and capable of exchanging data among satellite systems and services regardless of system size, ownership, or orbit.

[3] The authors acknowledge the difficulty in defining this term, for our purposes, conflict means the military is able to respond to kinetic and non-kinetic attacks.

[4] Hosmanek, A. J., Smith, B., & Dayton, M. (2022). *Law and Risk Management*. OpenHawks OER. https://pressbooks.uiowa.edu/introtolaw/chapter/law-and-risk-management/.

[5] Interview with Lt Gen (ret.) John Shaw, former Deputy Commander of US Space Command and Commander of US Space Force Space Operations Command (Potomac Institute for Policy Studies, Interviewer). (2025, December 10). [In-person]. For more, see: Potomac Institute for Policy Studies. (2026). *Making Space: Clearing the Way for Hybrid Architecture.* Potomac Institute for Policy Studies.https://www.potomacinstitute.org/reports/making-space-clearing-the-way-for-hybrid-architecture.

[6] Part of SmallSat Alliance HA definition in the *Making Space: Clearing the Way for Hybrid Architecture* report, March 12, 2026, https://potomacinstitute.org/reports/making-space-clearing-the-way-for-hybrid-architecture.

[7] *United States Space Force Space Warfighting: A Framework for Planners*. (2025). United States Space Force. https://www.spaceforce.mil/Portals/2/Documents/SAF_2025/Space_Warfighting_-_A_Framework_for_Planners_BLK2_(final_20250410).pdf.

[8] Department of Defense, 2019. "DoD Digital Modernization Strategy. Information Resource Management Strategic Plan FY2019-FY2023." *Department of Defense*. https://media.defense.gov/2019/jul/12/2002156622/-1/-1/1/dod-digital-modernizatino-strategy-2019.pdf; UK Ministry of Defence, 2021. "Digital Strategy for Defence: Delivering the Digital Backbone and Unleashing the Power of Defence's Data." April 2021. https://assets.publishing.service.gov.uk/media/60afae56d3bf7f435f43c7af/20210421_-_MOD_Digital_Strategy_-_Update_-_Final.pdf; CAF, 2022. "Canadian Armed Forces (CAF) Digital Campaign Plan". *Government of Canada*. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canadian-armed-forces-digital-campaign-plan.html.

[9] World Economic Forum. (2024). *Space: The $1.8 Trillion Opportunity for Global Economic Growth Insight Report*. https://www3.weforum.org/docs/WEF_Space_2024.pdf.

[10] *Introduction: An Assessment of U.S. Military Power*. (2026, March 4). The Heritage Foundation. https://www.heritage.org/military-strength/intro-assessment-us-military-power.

[11] Geneva Convention (III) Relative to the Treatment of Prisoners of War, art. 4(A)(4), Aug. 12, 1949, https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949/article-4.

[12] Joint Publication 1, Volume 2, Chapter IV, Section A, Paragraph 5.

[13] Kelton, M., Sullivan, M., Rogers, Z., Bienvenue, E., & Troath, S. (2022). Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States. *International Affairs*, *98*(6), 1977–1999. https://doi.org/10.1093/ia/iiac226

[14] The Canadian Armed Forces' Digital Campaign Plan (2022) as cited in Vasilescu (2025).

[15] Examples of these laws might include: the Law of Armed Conflict (LOAC), which governs the use of force in conflict; the Outer Space Treaty, which governs activities in outer space; and elements of federal acquisition law that govern how services are acquired, such as the principle that inherently governmental functions may not be contracted out to the private sector.

[16] Lt Gen (ret.) Tim Fay, Former Director of Staff for the Department of the Air Force, interview, Feb 2026
[17] Pernot, C. R. (2007, May 17). *The NSA and the Telecoms*. PBS. https://www.pbs.org/wgbh/pages/frontline/homefront/preemption/telecoms.html.
[18] Companies Act of 2006, 46 § 172 (2007). https://www.legislation.gov.uk/ukpga/2006/46/section/172.
[19] Klein, J., J. (2025). *Space Warfare: Strategy, Principles and Policy* (Second). Routledge.
[20] United Nations Office for Outer Space Affairs. (2019). *International Space Law: United Nations Instruments*. United Nations. https://doi.org/10.18356/014c0e55-en.
[22] Mendenhall, E. (2018). Treating Outer Space Like a Place: A Case for Rejecting Other Domain Analogies. *Astropolitics*, *16*(2), 97–118. https://doi.org/10.1080/14777622.2018.1484650.
[23] Kraska, J., & Pedrozo, R. (2023). Newport Manual on the Law of Naval Warfare. *International Law Studies*. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=3047&context=ils.
[24] United Nations General Assembly. (1966, December 19). *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*. United Nations Office for Outer Space Affairs. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html.
[25] Office of the General Counsel Department of Defense. (2016). *Department of Defense Law of War Manual*. https://apps.dtic.mil/sti/pdfs/AD1023075.pdf.
[26] Lt. Col. Matthew Zellner & Capt. Samantha Potter. (2025, August 22). *How Silicon Valley's Satellites Can be Targeted: Outer Space Law, Private Actors, and the Rise of the Civil-Military Relationship in Outer Space*. Stanford Space Law Society; Stanford Law School. https://law.stanford.edu/2025/08/22/how-silicon-valleys-satellites-can-be-targeted-outer-space-law-private-actors-and-the-rise-of-the-civil-military-relationship-in-outer-space-2/.
[27] Dunlap, C. (2021, March 5). Are Commercial Satellites Used for Intelligence-Gathering in Attack Planning Targetable? *Lawfire*. https://sites.duke.edu/lawfire/2021/03/05/are-commercial-satellites-used-for-intelligence-gathering-in-attack-planning-targetable/.
[28] The Defense Production Act of 1950, Pub. L. No. 81–774, 50 USC (1950). https://www.congress.gov/crs-product/R43767.
[29] Title 50, 1950.
[30] Baker, J. (2021). A DPA for the 21st Century (pp. 15–16). Center for Security and Emerging Technology. https://cset.georgetown.edu/publication/a-dpa-for-the-21st-century/.
[31] Office of the General Counsel Department of Defense, 2016.
[32] Office of the General Counsel Department of Defense, 2016.
[33] Office of the Secretary of Defense. (2023). *A Review of Space Acquisition*. Defense Business Board. https://dbb.defense.gov/Portals/35/Documents/Reports/2024/FY24-01%20-%20Space%20Acquisition%20Report.pdf.
[34] Koplow, D. A. (2021). *Reverse Distinction: A U.S. Violation of the Law of Armed Conflict in Space* [SSRN Scholarly Paper]. Social Science Research Network. https://papers.ssrn.com/abstract=3810975.
[35] Koplow, 2021.
[36] United States Department of Defense. (2024). DoD Commercial Space Integration Strategy. https://www.spaceforce.mil/Portals/2/Documents/Space%20Policy/USSF_Commercial_Space_Strategy.pdf.
[37] United States Department of Defense. (2024). *Department of Defense Commercial Space Integration Strategy*. https://media.defense.gov/2024/Apr/02/2003427610/-1/-1/1/2024-DOD-COMMERCIAL-SPACE-INTEGRATION-STRATEGY.PDF.
[38] Maj. Adam S. Reitz. (2024). *Operational Law Handbook*. The Judge Advocate General's Legal Center & School. https://tjaglcs.army.mil/Portals/0/Publications/Deskbooks%20and%20Handbooks/2024%20Operational%20Law%20Handbook%20(2024).pdf.

[39] Fergusson, Dr. J. (2005). Shall We Dance? The Missile Defence Decision, NORAD Renewal, and the Future of Canada-US Defence Relations. *Canadian Military Journal*, *6*(2), 13–22.
[40] Office of the General Counsel Department of Defense, 2016.
[41] Harrison, K. (2025, July 2). Satellite Insurance Plummets as Operators Skip Coverage. *Orbital Today*. https://orbitaltoday.com/2025/07/02/satellite-insurance-plummets-as-operators-skip-coverage/.
[42] Kollewe, J. (2026, March 2). Maritime Insurers Cancel War Risk Cover in Gulf as Iran Conflict Disrupts Shipping. *The Guardian*. https://www.theguardian.com/business/2026/mar/02/maritime-insurers-war-risk-cover-gulf-iran-shipping-strait-of-hormuz.
[43] Government Accountability Office. (2016). *Principles of Federal Appropriations Law* (GAO-16-463SP). https://www.gao.gov/assets/gao-16-463sp.pdf.
[44] Federal Tort Claims Act, Pub. L. No. 100–694, 28. https://www.law.cornell.edu/uscode/text/28/2680.
[45] Dover, A. P., & McGovern III, T. L. (2007). Risk Mitigation Approaches For Government Contractors. *Briefing Papers*, *07*(5), 1–16.
[46] Proprietary Contractor Data and Rights in Technical Data, Pub. L. No. 116–283, 10 (2021). https://uscode.house.gov/view.xhtml?path=/prelim@title10/subtitleA/part5/subpartD/chapter275&edition=prelim.
[47] Zirpoli, C. T. (2023). *An Introduction to Trade Secrets* (No. IF12315). Congressional Research Service. https://www.congress.gov/crs-product/IF12315.
[48] Elledge, B. H., & Elling, T. L. (2021, June 4). Federal Circuit Affirms Contractors' Ownership Rights in Technical Data and Trade Secrets. *Holland & Knoght Trade Secrets Blog*. https://www.hklaw.com/en/insights/publications/2021/06/federal-circuit-affirms-contractors-ownership-rights-in-tech-data.
[49] Lin, V. P. (2018, March 13). Commercial Space Race Highlights Differences Between Patent And Trade Secret Protection. *Whitimyer IP Group*. https://www.whipgroup.com/blog/commercial-space-race-highlights-differences-between-patent-and-trade-secret-protection/.
[50] Whitten, R., Wang, J., & Goldberg, J. (2026). Space Rules, or. . . Space Rules!: Reduced Export Controls Ease Cross-Border Collaborations (Part I of IV). *The National Law Review*, *XVI*(84). https://natlawreview.com/article/space-rules-or-space-rules-reduced-export-controls-ease-cross-border-collaborations.
[51] Japan Ministry of Economy, Trade, and Industry. (2025, January). *Security Export Guidance*. https://www.meti.go.jp/policy/anpo/seminer/shiryo/guidance_english.pdf.
[52] Ministère de l'Europe et des Affaires étrangères. (2019, December). *Export Controls on War Material*. France Diplomacy - Ministry for Europe and Foreign Affairs. https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/disarmament-and-non-proliferation/trade-transport-and-export-of-arms-and-sensitive-material/article/export-controls-on-war-material.
[53] *IP and Data Rights: Protecting DoD's Access to Innovation*. (2025). National Defense Industrial Agency. https://www.ndia.org/-/media/sites/ndia/policy/ip-and-data-rights/ip-and-data-rights-white-paper.pdf.
[54] Oakley, S. (2025). *Weapon System Sustainment: DOD Can Improve Planning and Management of Data Rights* (GAO-25-107468). Government Accountability Office. https://www.gao.gov/assets/gao-25-107468.pdf.
[55] Carpenter, D. H., & Ruane, K. A. (2018). *Selected Legal Tools for Maintaining Government Contractor Accountability* (No. R45322). Congressional Research Service. https://www.congress.gov/crs_external_products/R/PDF/R45322/R45322.1.pdf.
[56] Clark, S. (2025, April 4). *With New Contracts, SpaceX Will Become the US Military's Top Launch Provider*. ARS Technica. https://arstechnica.com/space/2025/04/with-new-contracts-spacex-will-become-the-us-militarys-top-launch-provider/.
[57] King, L. (2014, July 16). *McCain Dresses Down Senior Air Force General for Comments*. AZcentral. https://www.azcentral.com/story/news/politics/2014/07/16/mccain-dresses-down-air-force-general-

comments/12748363/?gnt-cfr=1&gca-cat=p&gca-uir=false&gca-epti=z1139xxe1139xxv000028&gca-ft=130&gca-ds=sophi.

[58] McClintock, B., & Glickstein, D. (2026). *Exploring Duality in Space* [Research Report]. RAND. https://www.rand.org/pubs/research_reports/RRA4003-2.html.

[59] Saideman, S. M., & Auerswald, D. P. (2012). Comparing Caveats: Understanding the Sources of National Restrictions upon NATO's Mission in Afghanistan1: Comparing Caveats. *International Studies Quarterly*, *56*(1), 67–84. https://doi.org/10.1111/j.1468-2478.2011.00700.x.

[60] Katze, J., & Kashgar, M. (2019). Legal Challenges in Multinational Military Operations: The Role of National Caveats. In *The "Legal Pluriverse" Surrounding Multinational Military Operations* (pp. 400–405). Oxford University Press. https://doi.org/10.1093/oso/9780198842965.003.0020.

[61] Katze & Kashgar, 2019.

[62] Theohary, C. A. (2024). *Use of Force in Cyberspace* [In Focus]. Congressional Research Service. https://www.everycrsreport.com/files/2024-11-29_IF11995_f2b460ebc9df5b256b66383002b4a465dab455f1.pdf.

[63] Cruz Cain, M. (2024). *Urgent Action Needed to Address Critical Cybersecurity Challenges Facing the Nation* (Report to Congressional Addressees GAO-24-107231). Government Accountability Office. https://www.gao.gov/assets/gao-24-107231.pdf.

[64] Schmitt, M. N. (February 20178). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Second). Cambridge University Press. https://www.cambridge.org/universitypress/subjects/law/humanitarian-law/tallinn-manual-20-international-law-applicable-cyber-operations-2nd-edition.

[65] Kanehara, A. (2022). Reconsideration of the Distinction between the Use of Arms in Law Enforcement and the Use of Force Prohibited by International Law —With an Analysis of the Inherent Significance of This Issue to Japan—. *Japan Review*, *5*, 13–48.

[66] Heinze, E. A. (2024). *International Law, Self-Defense, and the Israel-Hamas Conflict*. https://publications.armywarcollege.edu/News/Display/Article/3706538/international-law-self-defense-and-the-israel-hamas-conflict/.

[67] Blessing, J. (2026). *Never Trust, Always Verify* (No. 20260223–01). Potomac Institute for Policy Studies. https://www.potomacinstitute.org/files/Never%20Trust%20Always%20Verify_Improving%20Cybersecurity%20in%20Hybrid%20Architectures%20for%20Space.pdf.

[68] Hinnershitz, S. (2022, February 7). *Supplying Victory: The History of Merchant Marine in World War II*. https://www.nationalww2museum.org/war/articles/merchant-marine-world-war-ii.

[69] Lend-Lease Act, H.R. 1776 (1941). https://www.archives.gov/milestone-documents/lend-lease-act.

[70] Title 50, 1950.

[71] Title 46 of the CFR -- Shipping, Pub. L. No. 109–304, 46 (2006). https://www.ecfr.gov/current/title-46.

[72] United States Department of Transportation. (2024, February 23). *Civil Reserve Airfleet*. https://www.transportation.gov/mission/administrations/intelligence-security-emergency-response/civil-reserve-airfleet-allocations.

[73] United States Department of Defense. (2021, August 22). *Department of Defense Activates Civil Reserve Air Fleet to Assist With Afghanistan Efforts*. https://www.war.gov/News/Releases/Release/Article/2741564/department-of-defense-activates-civil-reserve-air-fleet-to-assist-with-afghanis/.

[74] United States Department of Transportation. (2025, June 16). *Voluntary Intermodal Sealift Agreement (VISA)*. https://www.maritime.dot.gov/national-security/strategic-sealift/voluntary-intermodal-sealift-agreement-visa.

[75] *Delta Air Lines, Inc.* (n.d.). GovTribe. Retrieved March 27, 2026, from https://govtribe.com/vendors/delta-air-lines-inc-dot-delta-airlines-7a344.

[76] Federal Aviation Administration. (2024, May 21). *Aviation Insurance Program*. https://www.faa.gov/about/office_org/headquarters_offices/ash/ash_programs/aviation_insurance.
[77] McLaughlin, R. (2019, June 18). The Legal Status and Characterisation of Maritime Militia Vessels. *European Journal of International Law*. https://www.ejiltalk.org/the-legal-status-and-characterisation-of-maritime-militia-vessels/.
[78] Office of the General Counsel Department of Defense, 2016.
[79] CTECH. (2025, June 20). *Iran Targets Microsoft Be'er Sheva Offices, Damages Residential Complex*. https://www.calcalistech.com/ctechnews/article/bkdal00geeg?ref=forever-wars.com.
[80] Kalia, S., Soni, A., & Dey, M. (2026, March 3). Amazon Cloud Unit's Data Centers in UAE, Bahrain Damaged in Drone Strikes. *Reuters*. https://www.reuters.com/world/middle-east/amazon-cloud-unit-flags-issues-bahrain-uae-data-centers-amid-iran-strikes-2026-03-02/.
[81] Office of the General Counsel Department of Defense, 2016.
[82] United States Department of Defense. (2019). *DoD Digital Modernization Strategy Information Resource Management Strategic Plan FY2019-FY2023*. https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF.
[83] Kowitt, B. (2019, May 17). *Inside Google's Civil War*. Fortune. https://fortune.com/longform/inside-googles-civil-war/.
[84] Vasilescu, C. (2025). Digital Transformation of Military Organisations. *Obrana a Strategie (Defence & Strategy)*, *25*, 25. https://doi.org/10.3849/1802-7199.25.2025.02.25-47.
[85] Simonite, T. (2021, November 18). *3 Years After the Maven Uproar, Google Cozies to the Pentagon*. WIRED. https://www.wired.com/story/3-years-maven-uproar-google-warms-pentagon/.
[86] Hoijtink, M., & Planqué-van Hardeveld, A. (2022). Machine Learning and the Platformization of the Military: A Study of Google's Machine Learning Platform TensorFlow. *International Political Sociology*, *16*(2). https://dx.doi.org/10.1093/ips/olab036.
[87] Vann, A. (2023). *The Takings Clause of the Constitution: Overview of Supreme Court Jurisprudence on Key Topics* (No. R47562). Congressional Research Service. https://www.congress.gov/crs_external_products/R/PDF/R47562/R47562.1.pdf.
[88] Staring, L. G. S. (1953, May). *The Mobilization of Shipping for War*. United States Naval Institute. https://www.usni.org/magazines/proceedings/1953/may/mobilization-shipping-war.
[89] See, e.g., Hust v. Moore-Mccormack Lines, 328 U.S. 707 (1946).
[90] Allen, D., Curl, M., & Allen, M. (2026, February 16). *Exclusive: Pentagon Warns Anthropic Will "Pay a Price" as Feud Escalates*. Axios. https://www.axios.com/2026/02/16/anthropic-defense-department-relationship-hegseth.
[91] Bordelon, B. (2026, March 5). *Pentagon Formally Designates Anthropic a Supply-Chain Risk*. POLITICO. https://www.politico.com/news/2026/03/05/pentagon-tells-anthropic-it-has-designated-the-company-a-supply-chain-risk-00814758.
[92] Eastland, M., Manson, K., & Turner, N. (2026, March 6). *Anthropic Vows Legal Fight Against Pentagon Sanction in AI Feud*. Los Angeles Times. https://www.latimes.com/business/story/2026-03-06/anthropic-vows-legal-fight-against-pentagon-sanction-in-ai-feud.
[93] Saideman & Auerswald, 2012.
[94] Lostumbo, M. J., McNerney, M. J., Peltz, E., Eaton, D., & Frelinger, D. R. (2013). *Overseas Basing of U.S. Military Forces: An Assessment of Relative Costs and Strategic Benefits*. Rand Corporation.
[95] Katze & Kashgar, 2019.
[96] Mamediieva, G., & Moynihan, D. (2023). Digital Resilience in Wartime: The Case of Ukraine. *Public Administration Review*, *83*(6), 1512–1516. https://doi.org/10.1111/puar.13742.
[97] Vasilescu, 2025.
[98] Glanville, L., & Pattison, J. (2024). Ukraine and the Opportunity Costs of Military Aid. *International Affairs*, *100*(4), 1571–1590. https://doi.org/10.1093/ia/iiae122.
[99] Hart, O. (2017). Incomplete Contracts and Control. *American Economic Review*, *107*(7), 1731–1752. https://doi.org/10.1257/aer.107.7.1731.

Potomac Institute for Policy Studies

Science for Policy. Policy for Science.

Targets, Treaties, and Trade Secrets: Understanding Space Hybrid Architecture's Legal Challenges

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

In collaboration with The Institute for National Strategic Studies

901 N. Stuart Street, Suite 1200
Arlington, Virginia 22203
Phone: (703) 525-0770

www.potomacinstitute.org

www.potomacinstitute.org

901 N. Stuart Street
Suite 1200
Arlington, VA 22203
(703) 525-0770

SCHOLAR PAPER SERIES
Issues in: Space
Paper Number: 20260415-01