THE ARSENAL OF DEMOCRACY

TECHNOLOGY, INDUSTRY, AND DETERRENCE IN AN AGE OF HARD CHOICES

EYCK FREYMANN
HARRY HALEM

FOREWORD BY ADMIRAL JAMES O. ELLIS JR., USN (RET.), AND NIALL FERGUSON

9

SPACE POWER

Space power has been critical to US military power since the Cold War, enabling operational integration across the air, land, sea, and cyber domains. Rapid advancements in launch technology and satellite design have democratized space over the past thirty years, making it increasingly accessible to other powers and reinforcing its centrality to US military capacity. The United States relies on three critical space-based capabilities: intelligence, surveillance, and reconnaissance (ISR) networks that provide comprehensive battlefield awareness; communications networks that enable global command-and-control (C2); and positioning, navigation, and timing (PNT) satellites that support precision weapons and navigation.[1] These services also support essential civilian functions. For example, PNT services—delivered by the GPS (global positioning system) constellation and foreign clones like BeiDou, GLONASS, Galileo, and so on—support banking, cell tower functioning, and a myriad of other essential functions for the civilian economy.[2]

US space systems are the world's best, making them attractive—and vulnerable—targets. Disruption to these systems could cripple US ISR, precision targeting, and command-and-control functions in a conflict, particularly in the Indo-Pacific. Recent People's Liberation

Army (PLA) tests of co-orbital satellites capable of maneuvering near US assets underscore the immediacy of the threat.[3] China's 560 percent growth in orbital assets since 2015, coupled with its demonstrated antisatellite capabilities, continues the long-term transformation of the space domain into an area of direct strategic competition.[4] The PLA's development of space-oriented directed-energy and cyber weapons, including ground-based laser systems capable of damaging satellite sensors, adds another layer of risk.[5] Norms against the testing of antisatellite (ASAT) weapons have created a generally benign environment for commercial activity in space. However, aggressive behavior by Russia and China and indiscriminate kinetic testing threaten to erode these norms.[6] Maintaining an adaptive advantage in the space domain has therefore become a critical priority from the perspective of US strategic deterrence.

Maintaining credible deterrence in space requires a multilayered defense strategy that combines cyber, electromagnetic, and kinetic protections. Cyber defenses protect satellite control systems from hacking or the insertion of malicious software that could compromise vital military communications. Electromagnetic spectrum management employs advanced signal control methods and antijamming technology to maintain communications in contested environments where adversaries attempt to jam signals. Kinetic protections guard against direct attacks on satellites by dispersing networks across multiple orbits and creating backup constellations, building resilience through redundancy. This layered approach helps ensure continued access to essential space-based services, even under attack.

Maintaining US technological superiority in space also increasingly requires leveraging allied partnerships while simultaneously protecting critical technologies from espionage. One promising approach involves creating resilient "mesh networks" of small satellite constellations in low-earth orbit (LEO), distributed across multiple orbital planes and shared by trusted allies and the civil space industry. Beyond hardware collaboration, US diplomacy can expand cooperation among democratic allies to confront Russian and PRC antisatel-

lite threats while jointly developing crucial emerging technologies. These include quantum communications for secure transmissions, advanced sensors and analytics, space nuclear propulsion for enhanced maneuvering, and in-space servicing capabilities to prolong satellite life. Such partnerships could help distribute the substantial costs and technical expertise required for effective space deterrence.

A Domain with No Good Analogy

In this book, we have used various historical analogies to help understand the future of combat in the Pacific. Analogies are never exact. History is the domain of contingency, and warfare is an explicitly nonlinear, chaotic phenomenon, with no consistent link between inputs and outputs.[7] Still, by considering multiple analogies together, it is often possible to draw inspiration even though no single analogy addresses all parts of the question.

This analytical approach fails in the space domain—and there is not even a canonical theory to fall back on. Modern naval thought owes a debt to the foundational writings of theorists such as Grotius, Mahan, and Corbett, even as subsequent thinkers like Wylie and Hughes, have adapted and occasionally broken with their ideas.[8] The theory of land power, and the general theory of warfare, owe a debt to Clausewitz and Jomini, the nineteenth century's two most notable military theorists, and implicitly draws off centuries of prior theorizing.[9] Since the early twentieth century, theorists from Douhet and Trenchard to Mitchell, de Seversky, and more recently Warden have proposed theories of airpower.[10] Some of these theories were too optimistic, but they provide a language and framework that military analysts, officers, and policymakers can use to think about air operations and their connection to strategy.[11]

By contrast, there exists only a handful of attempts at a comprehensive and robust theory of space power in the open-source literature.[12] What writings do exist are very recent and deal with only parts of the

broader space domain, such as the governance of celestial bodies and the role of space in communications. Following the creation of the US Space Force in 2019, an officer-training structure is being created independent from the Air Force. The US military published its first definition of "space power" in late 2020.[13] In time, specialized journals and presses will emerge and the conceptual vocabulary of space power will be refined. Some work on these questions probably exists in the classified domain. For now, however, the available literature is mainly focused on technical rather than theoretical issues.

Our own crude theory of space power would go something like this. Unlike land, sea, or airpower—each tied to territorial control or physical presence—space power is fundamentally about the control of information and connectivity across vast and largely empty space. Land power relies on holding territory, sea power on controlling sea lanes, and airpower on swift, localized force projection, but space power emphasizes the continuity of global communications, surveillance, and timing infrastructures that span the entire earth. Naturally, there are geographically tagged space "commands" subordinated to each geographic combatant command, but space assets are far more interconnected than those of other domains. In this sense, space power is about creating and sustaining an interconnected network that allows for real-time situational awareness, precision targeting, and uninterrupted command and control across all domains. Its value lies in enabling and supporting terrestrial operations, providing strategic oversight, and—through the dual-use nature of space assets—serving as a force multiplier for kinetic military power.[14]

Rather than projecting dominance through physical occupation, space power achieves deterrence through redundancy, survivability, and the ability to disrupt adversary networks if necessary.[15] There are, and will increasingly be, kinetic capabilities in orbit that relate to space operations, but they are part of a much broader military balance that includes non-kinetic elements as well. This theory suggests that in space, resilience and deterrence rest on ensuring that critical systems can withstand or recover from a range of emerging threats, including

orbital debris, electronic warfare, and cyberattacks. As the space domain becomes increasingly commercialized, the interplay between military and civilian space infrastructure will also grow in importance.[16] Space power will need to account for this evolving landscape, while also grappling with important ethical considerations around the militarization of space and the potential global consequences of space-based conflicts.

If this theory is any guide, then historical analogies from other domains are unlikely to be perfectly instructive—but we can briefly trace the evolution of space power to better understand the technological and strategic trends that have driven its development in the past.

Purpose-built weapons that transit the space domain emerged near the end of World War II. Germany's V-2 rocket, the world's first ballistic missile, was the first man-made vehicle to cross the Kármán Line, 100 kilometers above sea level—the formal edge of outer space. The Soviets and the Americans adopted German rocket technology, leading first to the USSR's launch of Sputnik in 1958 and subsequently to the space race.[17] The competition to place advanced assets in orbit was intimately connected to the Soviet and American nuclear weapons and ballistic missile programs.[18] A landmark in the history of space governance was the 1967 Outer Space Treaty (OST), which prohibits the placement of weapons of mass destruction in space. The OST does not cover conventional weapons or ballistic missiles that transit space. It did establish an enduring norm that space would be a peaceful domain. Except for the Reagan administration's Strategic Defense Initiative, no major power has publicly considered placing conventional weapons in space.[19] Russia may be considering breaking this norm by placing a nuclear device in space, although its progress is currently unclear.[20]

As we saw in chapters 1 and 2, satellites have been central to US military operations since the 1970s. The United States and the Soviet Union conducted aerial reconnaissance of each other's homelands, at first to detect nuclear bomber sites and over time to gather intelligence on nuclear-armed ballistic missile bases, troop movements,

and industry. Washington's answer to Sputnik was the U-2 spy plane, which flew above Soviet radar. However, the Soviets developed surface-to-air missiles capable of shooting the U-2 down, as it demonstrated in prominent incidents in 1960 and 1962. In response, the United States developed the first spy satellites.[21] It launched its first (then-classified) communications satellites in June 1966 and a series of second-generation launches began in November 1971.[22] Secure and low-signature communications with other services were enormously helpful for US Navy operations and greatly strengthened US nuclear deterrence in the 1980s. GPS was developed concurrently to support the American national security capabilities, including the nuclear deterrent.[23]

By the 1980s, both the Americans and the Soviets had deployed classified spy satellites that provided highly accurate imaging. The United States, however, gained a decisive advantage in the use of satellites for tactical communications and PNT, thanks to its growing lead in radio-frequency chips and other technologies. With a world-leading accurate PNT system, American nuclear-armed submarines could remain hidden until moments before launching their weapons and then update their inertial navigation targeting data with an accurate GPS signal.

Space assets in the early 1990s were relatively simple by today's standards, but they revealed their impressive capabilities in the Gulf War. As discussed in chapter 6, US air-naval forces deployed precision-guided weapons against Iraqi targets by using satellites for targeting and communications, while US and coalition ground forces swept through the vast Iraqi desert by using GPS navigation, catching Iraqi forces by surprise. Space-based command-and-control improved during the Global War on Terror. Today, all major militaries have become increasingly dependent on satellite technology for their essential functions, including surveillance and reconnaissance, PNT, communications, and command-and-control. The United States has grown particularly dependent on its space-based systems to support its global force posture. Our economy and society have developed a critical dependence on space infrastructure that the US government may lack the means to protect and defend.

In the 2000s, great-power competition began to intensify in space in both the civilian and military domains—but at the same time, commercial activity in space began to boom. The Trump administration established the US Space Force in December 2019 in recognition of these two interrelated trends. In 2024, John Plumb, assistant secretary of defense for space policy, testified to Congress that Russia is developing a "new satellite carrying a nuclear device" that "could pose a threat to all satellites operated by countries and companies around the globe, as well as to the vital communications, scientific, meteorological, agricultural, commercial, and national security services we all depend upon."[24] He added that a nuclear detonation would likely render the LEO unusable for at least a year.[25] Despite these extreme scenarios, space will likely remain primarily a zone for reconnaissance and communications for the foreseeable future. Weapons placed in space will prioritize attacking specific enemy reconnaissance and communications satellites rather than ruining the entire LEO.

Lessons from Ukraine

The Russia-Ukraine war serves as an instructive example of how satellite technology has transformed the battlefield by enhancing communication, coordination, and targeting capabilities, while also introducing new critical vulnerabilities.

When Russia invaded Ukraine in early 2022, Ukraine had limited accessible space assets. Those that existed were almost immediately taken offline through Russian jamming. Nevertheless, Ukraine quickly integrated SpaceX's Starlink into its operations. Using truck-mounted terminals powered by small generators, Ukrainian forces maintained vital communications and real-time coordination, gaining a significant intelligence advantage over Russian forces. Starlink's LEO constellation provided reliable connectivity in rural areas and enabled real-time targeting adjustments through drone video feeds to artillery units—a capability reportedly crucial in the Ukrainian drone

attack on Russia's Black Sea Fleet at Sevastopol.[26] As Ukraine's minister of Digital Transformation noted, Starlink became "the blood of our entire communication infrastructure."[27] US-based companies like Maxar have provided additional support through high-resolution battlefield imagery, notably revealing the devastation of Bucha in 2022.[28]

However, reliance on commercial satellite systems has exposed new vulnerabilities. In February 2022, Russia successfully disrupted Ukrainian communications through a cyberattack on Viasat's ground infrastructure. This attack highlighted how terrestrial systems have obvious vulnerabilities, though it is notable that the network was repaired and functioning again within three days.[29] Both sides have attempted to interfere with GPS and GLONASS signals, recognizing that positioning and timing services are essential for guided munitions and unmanned systems.[30] More fundamentally, because Ukraine's satellite network is not sovereign, it must rely on foreign operators to allow it to access satellite coverage. Elon Musk has enjoyed an explicit veto over potential Ukrainian operations in the Black Sea and against Russian territory.[31]

As discussed, the Russia-Ukraine war has highlighted two significant trends in space warfare: proliferation and commercialization. The proliferation of satellites, including mega-constellations like Starlink, provides resilience by reducing reliance on individual critical systems and complicating adversaries' antisatellite efforts. Yet Ukraine's reliance on commercial space services has also transformed the civil-military relationship.[32] As private firms become indispensable to military operations, the reliance on civilian technology could lead governments to reconsider regulatory practices and contracting approaches to secure operational autonomy in future conflicts.[33]

China's Space Strategy

Since the Gulf War, PLA sources have recognized US space assets as the key enabler of American military power, resolving to use asymmetrical

strategies to close the gap and compete in the space domain.[34] Authoritative PRC sources describe space as the "ultimate high ground," framing space warfare as inevitable.[35] PLA documents make frequent comparisons between nuclear and space-based capabilities, identifying space as a "more usable and effective" medium for coercion.[36] This strategic orientation allows China to use space to signal high-stakes deterrence without requiring nuclear escalation, as space capabilities can directly threaten an adversary's infrastructure.[37] Thus, PLA strategists anticipate that space and counter-space capabilities will play an "outsized role" in strategic coercion, proving potentially more practical than nuclear or conventional threats in influencing adversarial behavior.[38]

Under Xi, dual-use space technologies have become a central priority for PRC industrial policy. Made in China 2025 identifies space as one of ten major priority sectors, while the 14th Five-Year Plan (2021) highlights space as a focus area.[39] Within this framework, China's Project 221 integrates advancements in human space flight, lunar exploration, next-generation launch vehicles, and satellite navigation—all key to PLA strategic objectives.[40] China's BeiDou navigation system, ostensibly civilian, supports PLA missile targeting in the Indo-Pacific, underscoring how Made in China 2025 and other initiatives are blurring the lines between civilian and military space capabilities.[41]

As China pursues deep space exploration programs for status reasons, its top space priorities concern information networks that fulfill PLA objectives.[42] In 2023, China placed 217 payloads into orbit, with over half of them serving to strengthen the PLA's intelligence, surveillance, and reconnaissance (ISR) network. China now boasts over 490 ISR satellites that will enable the PLA to detect American assets in the Indo-Pacific.[43] The Space-Earth Integrated Information Network Mega Project, launched in 2017, is a prime example. China Satellite Network Group is also developing a national broadband mega-constellation, akin to a state-operated Starlink, to expand communication capabilities.[44] Space appears to be a personal priority for Xi, who promoted two former leaders of China's space program—Ma

Xingrui and Yuan Jiajun—to prominent regional posts as party secretaries in Xinjiang and Chongqing, respectively.[45]

China's focus on space technology has already produced significant results. The PLA has demonstrated ground-based antisatellite (ASAT) capabilities, including missiles and lasers that can disable or blind US LEO satellites.[46] The development of a fractional orbital bombardment system, which involves ballistic missiles passing through LEO orbit en route to their targets, showcases China's progress in advanced strike technologies.[47] In 2021, China's Tianwen mission reached Mars, making it the fifth country to orbit the planet and the first to conduct an orbiter-lander-rover mission simultaneously.[48] Investment in expanding the BeiDou system has further reduced China's reliance on the US-controlled GPS, aligning with PRC strategic imperatives.[49]

Looking ahead, Xi is likely to keep space a priority throughout his tenure. His administration has set ambitious goals: by 2030, China aims to become a "major space power" and a "fully comprehensive space power" by 2045.[50] Milestones include establishing orbital servicing, autonomous refueling systems, a Space-Earth Integrated Information Network, a national civil space infrastructure, and a manned lunar base. In 2020, Beijing and Moscow agreed to cooperate on a lunar research station, a project underscoring a growing alignment in space technologies between the two nations.[51] As Kevin Pollpeter observes, "Even if US space power continues to improve in absolute terms, China's rapid advance in space technologies will result in relative gains that challenge the US position in space."[52]

China's expanding cooperation with Russia in space technology further reinforces this strategic direction. Despite lingering Cold War–era distrust, China and Russia have made headway in space collaboration, maintaining separate navigation systems—BeiDou for China and GLONASS for Russia—while aligning on initiatives like antisatellite weaponry and space-related nuclear technology. Even if BeiDou and GLONASS remain distinct, their cooperative stance allows each country to coordinate in areas that challenge US space dominance.[53]

Antisatellite Warfare

In any potential conflict, US planners must assume that China may quickly turn to antisatellite warfare.[54] The current US space C2 infrastructure remains overreliant on a small number of key assets, creating single points of failure. In a conflict, PLA forces could exploit this vulnerability with simultaneous ASAT attacks and electronic warfare in an attempt to sever US C2 links.

Antisatellite warfare technologies vary based on the orbit of the satellite being targeted. Most communications, navigation, and spy satellites operate in LEO, 1,000–2,000 kilometers above sea level, or medium earth orbit (MEO), 2,000–35,000 kilometers above sea level.[55] In LEO, and to a lesser extent in MEO, it is relatively straightforward to interfere with satellites by dazzling them with lasers, physically disabling them with robotic devices, or striking them with projectiles.[56] In systems like Starlink, with its array of around 4,500 small, mobile satellites in LEO, while each satellite is relatively easy to jam, the network's sheer size makes collective disruption challenging. However, despite their resilience to direct interference, Starlink constellations remain vulnerable to cyberattacks and kinetic attacks on ground stations. In contrast, satellites operating in medium and geosynchronous/high earth orbit (35,000 kilometers and above) are much harder to disrupt. Because they are farther away, it takes far more power to jam their signals or dazzle them. However, satellites in MEO and geosynchronous orbit are typically larger, more expensive, more technically complex, and less responsive than lower satellites. Thus, they still face threats from emerging ASAT capabilities being developed by China, Russia, and North Korea.[57]

Alarmingly, Russia and China seem unafraid to publicly demonstrate or threaten ASAT techniques that involve kinetic strikes. China's 2007 kinetic antisatellite test created debris that threatened other countries' satellites.[58] Russia is developing the capability to use nuclear electromagnetic pulses (EMPs).[59]

Over the long term, accumulating space debris might even make it impossible for humanity to use the LEO, in a phenomenon known as the Kessler effect.[60] The next generation of kinetic ASAT weapons may be "kinetic kill vehicles"—essentially tiny satellites with small motors—that travel on motherships to get close to their targets. Even a very small object can do significant damage to a space-based platform, since objects in space move at enormous speeds. The hardest technical challenge is shifting orbits, which require large thrusters and complex design changes.

In the short to medium term, non-kinetic attacks such as cyberattacks and jamming arguably pose an even greater risk to US space systems. Kinetic attacks on satellites are difficult, expensive, slow, and easily attributed. Russia has demonstrated GPS-jamming techniques that do not destroy or degrade satellites but nevertheless greatly reduce the accuracy of precision-guided munitions.[61] Satellite ground control stations are also vulnerable to cyberattack.

Deterring Space Attacks

In the long run, it would be highly desirable to negotiate robust arms control agreements to limit the development of strategically destabilizing counter-space capabilities. For the moment, however, China and Russia have shown little desire to engage in good faith in such discussions.[62] The United States will probably not have the opportunity to establish future arms control agreements in space unless it can negotiate from a position of strength by establishing a decisive technological and operational lead. The United States and its allies must therefore show they can hold China and Russia's space systems at risk. The US does not have a publicly acknowledged antisatellite warfare program, but there are hints in open sources that it may have formidable secret capabilities. One notable system is the Boeing X-37B orbital space plane.[63] Maintaining an advantage in orbital space planes and related technologies should remain a priority. China recognizes

this and now has a space plane of its own.[64] Russia is particularly vulnerable to antisatellite warfare. Both Russia and China still use GPS for many civilian purposes. Russia's space program is particularly vulnerable to ASAT weapons, since it relies on legacy Soviet capabilities and Roscosmos is budget constrained.[65]

Still, even if the United States can respond in kind to attacks on its satellites, this may not be sufficient to retain deterrence.[66] For reasons of geography discussed in earlier chapters, the United States is more dependent on satellite targeting and communications in the Indo-Pacific than China. In a conflict, US forces would be fighting at sea, with assets dispersed across a wide area. By contrast, China could use medium-range long-endurance drones and long-range maritime patrol and strike aircraft for targeting if it lost its satellites. In theory, US forces could resort to undersea communications cables and long-distance radio to communicate, but undersea communications cables can be identified and cut. Returning to analog communications would be a doctrinal and cultural shock.[67] All modern militaries are shifting combat communications into space to rely less on airborne and surface assets that are vulnerable to long-range strike. The US Air Force, for example, plans to replace its manned E-8 Joint Surveillance Target Attack Radar System with a combination of unmanned systems and satellites.[68] These moves require a strategy to make the US satellite network resilient to attack, not just to hold adversaries' space assets at risk.

There are a few ways to defend actively against antisatellite warfare, but all have trade-offs.[69] It is theoretically feasible to install point defenses on satellites.[70] The Outer Space Treaty does not explicitly prohibit the placement of conventional weapons in space, though publicly revealing offensive military assets in space would trigger responses from US adversaries and almost certainly also US partners with space capabilities. US allies might be spooked, even though Russia may have already deployed weapons in space.[71] The United States could launch new satellites in higher orbits, but this is expensive and requires more sophisticated and expensive equipment

and software. The United States therefore needs to harden its existing space-based assets and create space-based, airborne, and terrestrial/undersea redundancies.[72]

The clearest path to making the US command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) network more survivable is to keep increasing the number and orbital diversity of US and allied satellites, particularly in LEO. If the cost of destroying a US satellite is higher than the cost of replacing it, China is unlikely to attack the network. LEO constellations also use smaller, more mobile operating stations, which makes the overall system more resilient to cyberattack.[73] As of July 2023, the Department of Defense had already awarded over $900 million in contracts through the Proliferated Low Earth Orbit Satellite-Based Services program to sixteen companies specializing in satellites in broadband, imaging, alternative PNT, and more.[74]

Private US firms already operate constellations of cheap satellites in LEO. Satellites in a constellation operate in a synchronized manner to ensure continuous coverage and data relay across large areas. Starlink operates an impressive constellation of around 4,500 satellites, with each satellite just a few dozen meters across and relatively cheap to replace.[75] China's direct-ascent antisatellite weapons would probably struggle to intercept them, given their size.[76] Maxar Technologies' WorldView imaging constellation consists of only six satellites, making it far more vulnerable to antisatellite warfare. The ultimate goal is to create a resilient and hardened satellite infrastructure to ensure its continuance even in extreme scenarios. By increasing investment in these technologies and leveraging private industry, the United States can build a satellite network capable of withstanding potential adversarial actions.

LEO satellites are advantageous because they are cheap and require relatively little power, but they also have drawbacks. Satellites in LEO can monitor a specific location on Earth for only about ten minutes, making continuous observation difficult.[77] As a result, the US defense and intelligence communities lack "constant stare" capability and

cannot track every relevant trend and abnormality.[78] Addressing this gap will require continued investment to expand the reconnaissance satellite fleet and efforts to distribute satellites across low, medium, and geostationary orbits to enhance coverage and increase system resiliency.[79] It is also important to ensure that satellite constellations follow diverse orbits. If large groups of satellites are located in the same orbital plane, they may be vulnerable to debris associated with the destruction of even a few satellites.[80]

In light of this discussion, the US and allied countries should maintain a space-industrial base capable of quickly replacing any satellites that are lost or damaged in conflict with China. In a wartime context, private firms would probably enter emergency contracts with the US government. Governments would likely cut red tape to optimize access to launch platforms and other systems. For a variety of reasons, it would be advantageous for the US to collaborate with allies and partners in this effort. Even though the US enjoys a decisive lead, Japan and the European Union have robust space capabilities, albeit with significant gaps.[81] Building a joint allied space-industrial base will require International Traffic in Arms Regulations (ITAR) reform.

Emerging Tech Trends

The rapid evolution of space technology is transforming both commercial and military operations. Five key areas—launch infrastructure, hybrid architectures, nuclear propulsion, in-space servicing, and advanced sensing—are advancing economic and military capabilities, but current operations remain constrained by traditional technologies. Emerging innovations in these domains could revolutionize US space capabilities and enhance deterrence by the 2030s, but realizing this potential depends on overcoming PRC countermeasures, system vulnerabilities, and evolving strategic priorities. Maintaining US leadership will require robust commercial investment, allied collaboration, and streamlined regulation.

Launch Infrastructure and Rocketry

Space launch capability is fundamental to US space power. The United States currently dominates global launch capacity, accounting for 81 percent of effective capacity and nearly half of all launches in 2023. However, existing infrastructure faces critical constraints.[82] Notably, Cape Canaveral and Vandenberg Space Force Base, designed initially for government-led missions, are nearing capacity limits for launches.[83] SpaceX has added a private site in Texas. This bottleneck could prove particularly problematic in scenarios that require rapid satellite replacement, especially in response to adversarial attacks or emergent needs.

In recent years, two key technological developments have reshaped launch capabilities. First, reusable rocket technology has drastically reduced launch costs, from $45,000 per kilogram in 1980 to approximately $1,500 today.[84] Advances in propulsive landing and heat shield technology allow multiple reuses of launch vehicles. Some boosters are now capable of over ten launches. High-cadence launch support will enhance resilience and adaptability in space.[85]

If current trends in launch technology continue, the next ten to fifteen years could see space operations fundamentally transformed. Launch costs might drop below $500 per kilogram by 2030 and potentially much lower by 2035 if fully reusable vehicles become standard.[86] This cost reduction, combined with a higher cadence of launch (potentially weekly or better from single pads), would enable rapid constellation deployment and replacement. The military implications could be significant. Distributed, redundant satellite networks would become more practical. Launch sites, rather than vehicles or costs, would become the primary constraint on space operations. This trend could reduce the strategic value of antisatellite weapons by making it easier and faster to replace satellites than to destroy them.

Regulation will be a key determinant of how fast launch costs fall. Launch licensing delays, environmental assessments, and range access limitations have created significant gaps between technical readiness

and operational deployment.[87] Both the Defense Innovation Unit (DIU) and the US Space Force have warned that launch demand may soon exceed available facilities, even as private companies continue to develop increasingly capable launch systems.[88] The strategic implications for deterrence are potentially substantial. Constraints in launch infrastructure could hamper the US ability to reconstitute space assets quickly during conflict, potentially undermining deterrence by signaling limited resilience in space. Streamlining licensing and regulatory processes relating to launch can likely be done without significant risks to safety and is necessary to preserve the US lead over great-power rivals in the short to medium term.

Hybrid Space Architectures

Hybrid space architectures integrate smaller commercial satellites with traditional government systems to create a resilient, networked environment across multiple orbital planes. Based on current designs such as the Space Development Agency's Proliferated Warfighter Space Architecture, maintaining minimal viable capability would require approximately four hundred to five hundred satellites in LEO.[89]

The war in Ukraine has highlighted both the potential and the limitations of hybrid space architectures. Commercial satellite communications (e.g., Starlink) have been essential for Ukrainian forces, while commercial imagery companies have provided real-time intelligence on Russian movements. However, these systems have been integrated on an ad hoc basis, which has also exposed vulnerabilities. To deter China, the US government should offer contracts to commercial operators to integrate them into its space architecture in advance of a conflict. The potential value for deterrence is high. Hybrid architectures offer immediate operational utility by providing resilience through redundancy. The technology is mature. The key is to scale these systems and ensure seamless integration between commercial and government assets.

Advanced Nuclear Power and Propulsion

Today's spacecraft propulsion systems rely on chemical rockets for high-thrust, short-duration burns or electric propulsion for low-thrust, long-duration orbital changes. However, both systems have limitations in terms of speed and payload capacity. Traditional photovoltaic systems for in-orbit operations are limited by solar exposure and not suitable for some deep-space missions.

Nuclear propulsion—particularly nuclear thermal propulsion (NTP), which harnesses heat from uranium atom bombardment—could provide rapid maneuverability and increased payload capacity in space.[90] This technology not only reduces reliance on solar energy but also potentially offers a thrust-to-weight ratio approximately ten thousand times greater than electric propulsion and up to five times more efficiency than in-space chemical propulsion.[91] As China develops its own nuclear propulsion capabilities, the competitive landscape in this field is intensifying.[92] The Defense Advanced Research Projects Agency (DARPA) and NASA have announced plans to test a nuclear engine in space by 2027 to support missions to Mars.[93] The US Space Force is actively backing this research and funding additional projects focused on nuclear reactor–powered propulsion technologies, recognizing their significant military applications.[94] The Joint Emergent Technology Supplying On-Orbit Nuclear Power (JETSON) project, supported by the Department of Energy, is one notable project in this space. In addition, the Defense Innovation Unit (DIU) has awarded contracts for developing small-scale nuclear batteries capable of powering spacecraft.

NTP's potential strategic value for deterrence is high. The ability to rapidly reposition assets or sustain operations in deep space could potentially provide the United States with decisive strategic advantages. However, although the basic science is highly promising, regulatory, safety, and classification hurdles will delay deployment.[95] Nuclear propulsion is subject to many classification challenges, particularly under ITAR and the Atomic Energy Act.[96] Even sharing sensitive

technical details with Five Eyes countries is challenging.[97] Current legal frameworks also don't adequately address how to deploy nuclear assets internationally or protect them from adversary interference. Addressing these barriers must be a priority if nuclear propulsion is to become operational within the next decade, and particularly if the United States and China find themselves in a race to deploy the technology.

In-Space Servicing, Assembly, and Manufacturing (ISAM)

Today, space systems must be fully assembled on Earth and launched in their final form, limiting their size, life span, and flexibility. ISAM aims to extend satellite life span and functionality by enabling robots to inspect, repair, refuel, and upgrade satellites in orbit. This would allow for the assembly of large structures that exceed rocket fairing dimensions and allow for continuous upgrades to space systems.

The rapid expansion of the space industry and the increase in launches have necessitated a parallel rise in replacement capacity to sustain satellite constellations. McKinsey estimates that by 2030, around twenty-seven thousand active satellites will orbit Earth, requiring four thousand to five thousand launches annually to sustain the constellations.[98] The United States is already making strides in ISAM: Lockheed Martin's In-Space Upgrade Satellite System (LINUSS) has successfully demonstrated proximity maneuvering and in-space servicing technologies,[99] while Northrop Grumman's Mission Extension Vehicle (MEV) has shown the potential for refueling and controlling aging satellites.[100] Foreign powers have made notable strides. For instance, China's Shijian-21 towed a dead satellite to a new orbit,[101] and Astroscale, a Japanese company, demonstrated its ability to magnetically capture another satellite.[102]

The dual-use nature of ISAM presents potentially serious risks. Any system capable of servicing a satellite could also potentially interfere with or disable it.[103] In contested space environments, such as LEO, maintaining positive control over ISAM vehicles will require

robust encryption, authentication protocols, and real-time monitoring to prevent adversary interference.

Moreover, the future of ISAM is fundamentally constrained by current launch limitations. Progress will require further advances in rocket reusability. Currently, only around 4 percent of a rocket's total mass is usable for the intended payload; the remaining 96 percent is taken up by fuel, engines, and structure.[104] Increasing rocket reusability can reduce costs and improve launch frequency, making it more economical to develop satellite servicing and upgrade capabilities.[105] Such advancements would help fulfill US Space Command's push for "Dynamic Space Operations"—that is, the ability to maneuver without thinking about fuel or life-span limitations.[106]

Advanced Sensing and Analytics

Space-based sensing and analytics have traditionally relied on a small number of highly specialized satellites, but emerging technologies in artificial intelligence/machine learning (AI/ML) and onboard data processing are rapidly changing this paradigm.[107] Advanced sensing and analytics can provide early warnings of adversary activity, especially from China, and offer real-time intelligence to decision-makers.

A vibrant commercial market for remote sensing already exists.[108] The operational and strategic value of remote sensing has also become increasingly evident. Commercial remote sensing technologies played a critical role in revealing Russia's buildup of armored columns along the Ukrainian border in late 2021, alerting the international community to Putin's intention to invade.[109] Since then, commercial imagery has documented the extensive destruction in Ukraine.[110] There remains significant potential for growth in the number of reconnaissance satellites and the resolution of satellite imagery, as well as deep learning to process and interpret the vast pools of remote sensing data.

Synthetic Aperture Radar (SAR) is a key innovation. Traditional optical satellite imaging struggles with cloud cover, darkness, and weather anomalies. SAR overcomes this problem by bouncing

microwave radar signals off the earth to detect physical properties and map the earth's surface. These signals are then collected and processed to remove noise and construct an image. Finally, the image is interpreted to identify objects or other meaningful information, often using AI.[111] The integration of AI can significantly enhance SAR systems by improving image quality, reducing noise, and facilitating automatic target recognition.[112] In other words, integrating AI with SAR could help analysts detect, classify, and track objects of interest, increasing reconnaissance and situational awareness. In early 2022, the US National Reconnaissance Office began purchasing commercial SAR imagery from six US firms.[113] These firms have also been crucial in providing SAR data to the US intelligence community to help support Ukraine.[114]

Although commercial advancements in remote sensing are promising and can contribute to deterrence, integrating them into military systems and overcoming current latency and data processing challenges will take time. The United States faces potential gaps in ground station coverage, particularly over the Pacific, which limits real-time data availability. In an effort to overcome these challenges, the US Naval Information Warfare Center (NIWC) Pacific recently entered into a $99.6 million contract with Northrop Grumman to develop a ground station in Guam. This will function as a relay point for missile warning signals between different satellite networks to overcome potential bandwidth issues.[115]

Quantum Communication and Cryptography

As the United States enhances its space operations, secure communications will be essential for maintaining an edge over adversaries. Quantum communication and quantum cryptography present the potential for highly secure communication channels. Unlike traditional encryption, the intrinsic nature of quantum interactions ensures that any unauthorized interference in a quantum communication is detectable.[116] China has already made significant strides in quan-

tum communication, including launching a quantum-enabled satellite, Micius, in 2016. This satellite successfully transmitted secure data using quantum key distribution (QKD),[117] achieving reduced signal loss compared with terrestrial optical fiber channels and enabling significantly faster information delivery.[118]

The implications of quantum communication are potentially strategically transformative. Secure, unhackable communication in space could support sensitive military and intelligence operations, particularly in command-and-control (C2) systems where secure transmission of orders and intelligence is essential. Satellite-based QKD could facilitate quantum-secure communication over vast distances.[119] However, there are significant challenges in the short term—particularly in space.[120]

As quantum computing rapidly advances, some experts believe that, within the next decade, we may see the emergence of quantum devices capable of breaking existing encryption methods.[121] The immediate threat to cybersecurity may not be urgent, but the potential for hostile actors to exploit quantum computing for decryption poses significant concerns for the protection of critical information, including national security data.[122] In response to the looming threat, the US Department of Commerce's National Institute of Standards and Technology (NIST) has released a set of encryption algorithms designed to withstand potential quantum cyberattacks. These new standards aim to establish robust data protection through algorithms for general encryption and digital signatures.[123]

Scaling is a key challenge. Expanding to a global quantum communications network, where satellites can communicate with multiple ground stations or with each other, would require significant advances in technology and infrastructure. Quantum communication over long distances is hampered by photon loss, making it difficult to maintain data integrity across thousands of kilometers. Quantum repeaters—devices that amplify quantum signals without disrupting their quantum state—are still under development. The development of ground stations capable of receiving quantum communications and distrib-

uting them across networks presents another bottleneck. These stations require specialized equipment to handle the transmission and reception of quantum-encrypted signals.[124]

Despite these challenges, major countries are investing heavily in quantum communication technology, with key demonstrations expected in the next decade. The United States has been proactive in funding initiatives critical to the DOD's focus on quantum sensing, encryption, and communications.[125] In May 2022, the Biden administration released the National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems (NSM-10), outlining specific actions for agencies to begin a multiyear transition to quantum-resistant cryptography.[126] Given China's investments in this domain, maintaining US leadership will require sustained research investment, industry partnerships, and realistic assessment of technical constraints.

Conclusion

As space technology has rapidly matured, space has become indispensable to US security and the broader global strategic balance. Yet, unlike air, land, and sea power, space power lacks a well-defined theory to guide its development. Based on the evolution of space power in recent decades, a crude theory would suggest a fundamentally different logic from that of other domains. Air, land, and sea power center on physical control and localized force projection in strategic territory, adjacent maritime and air space, and shipping routes. By contrast, space power is largely about the collection and secure transmission of information across vast empty spaces. Space power's core value lies in creating and sustaining a global network for real-time situational awareness, precision targeting, and uninterrupted command and control across domains. In this sense, it does not dominate through physical occupation but rather through resilience, survivability, and

the potential to disrupt adversary networks. In space, one achieves deterrence by ensuring that one's own systems can remain operational under a wide range of threats, while holding an adversary's systems at risk. As space power evolves, its conceptual evolution will accelerate as well, drawing insights from other domains where appropriate while still recognizing its unique capabilities, constraints, and realities.

The key challenge for US policymakers is to turn this emerging theory into a framework that contributes to deterrence against current and potential adversaries, including China. Investments in layered defenses—cybersecurity, electromagnetic spectrum protections, and distributed constellations—will be essential to building a space network that can endure in the face of adversarial attacks and the unpredictable hazards of space. Partnering with private-sector actors and maintaining and expanding the infrastructure for rapid satellite replacement will reinforce deterrence. Redundancy and reconstitution capabilities make the network robust against even sustained aggression. In addition, as the space domain grows more commercialized, collaboration with allies will become critical for establishing a secure allied space industrial base. Reforming ITAR would strengthen US and allied space architecture, laying the groundwork for a doctrine of joint resilience. Joint exercises and carefully calibrated counter-ASAT capabilities will support this doctrine, establishing credibility while avoiding uncontrolled escalation.

Developing a framework for space power must also mean leading diplomatically to establish norms around responsible conduct in space. The US should seek to build a "Space Stability Framework" that prioritizes transparency, limits ASAT testing, and ensures sustainable space traffic management. By shaping the foundational rules of space engagement, the US can guide space power toward stability and ethical governance, especially as commercial and military infrastructures become more intertwined.