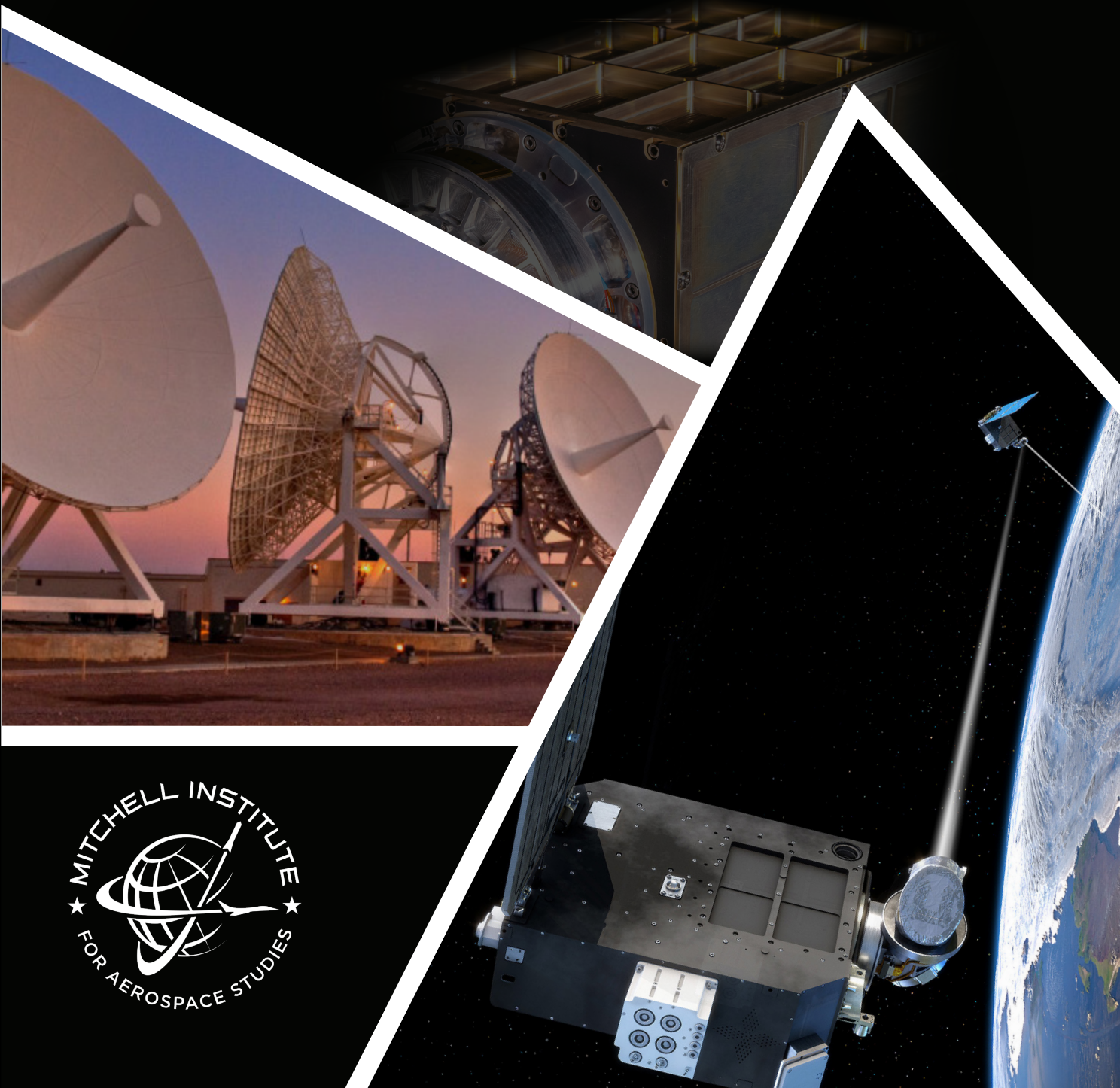


War at the Speed of Information:

Data Transport, Decision Advantage, & the Future of Military Space Communications

Col Jennifer K. Reeves, USAF (Ret.)



WAR AT THE SPEED OF INFORMATION: DATA TRANSPORT, DECISION ADVANTAGE, AND THE FUTURE OF MILITARY SPACE COMMUNICATIONS

Col Jennifer K. Reeves, USAF (Ret.)

The Mitchell Institute for Aerospace Studies
Air & Space Forces Association
Arlington, VA
September 2026

About the Mitchell Institute for Aerospace Studies

The Mitchell Institute for Aerospace Studies is an independent, nonpartisan policy research institute established to promote understanding of the national security advantages of exploiting the domains of air, space, and cyberspace. The Mitchell Institute's goals are: 1) to educate the public about the advantages of aerospace power in achieving America's global interests; 2) to inform key decision-makers about the policy options created by exploiting the domains of air, space, and cyberspace, and the importance of necessary investment to keep America the world's premier aerospace nation; and 3) to cultivate future policy leaders who understand the advantages of operating in air, space, and cyberspace. Mitchell Institute maintains a policy not to advocate for specific proprietary systems or specific companies in its research and study efforts.

About the Author

Col Jennifer Reeves, USAF (Ret.), is a Senior Resident Fellow for Space Studies at the Mitchell Institute's Spacepower Advantage Center of Excellence (MI-SPACE). Reeves retired from the U.S. Air Force as a Colonel with almost 29 years of active duty service, finishing her career as the Chief of the Air Force's Engine Room, leading the service's Program Objective Memorandum (POM) build. She previously commanded the 341st Missile Wing at Malmstrom Air Force Base, the 381st Training Group at Vandenberg Air Force Base, and the 2d Space Warning Squadron at Buckley Air Force Base. Reeves served on three headquarters staffs, was deployed or stationed in five combatant commands, and served on two general officer personal staffs. Reeves earned an Associate's degree equivalent from her German secondary school in Berlin, a Bachelor of Science in Aerospace Engineering from San Diego State University, a Master of Basic Science in Physics from the University of Colorado in Denver, and a Master of Strategic Studies from the Air War College.

Cover design by Kamilla Gunzinger

Image Credits: Artistic depictions and photos courtesy of GA-EMS and NASA.

Contents

FOREWORD	1
ABSTRACT	2
THE STRATEGIC CHALLENGE: LEGACY COMMUNICATIONS IN A DATA-INTENSIVE BATTLESPACE	3
LEGACY ARCHITECTURES WERE BUILT FOR A DIFFERENT ERA	3
OPERATIONAL DEMAND IS OUTPACING TRANSPORT CAPACITY	5
THE COST OF INACTION	7
WHY CURRENT APPROACHES ARE NO LONGER ENOUGH	8
MODERN WARFARE DEPENDS ON DECISION ADVANTAGE AT SPEED & SCALE	8
CONTESTED ENVIRONMENTS ARE HOSTILE TO LEGACY COMMUNICATIONS	10
DATA PRODUCTION IS RISING FASTER THAN LEGACY NETWORKS CAN ABSORB	13
STRATEGIC COMPETITION IS SHAPING THE FUTURE COMMUNICATIONS ENVIRONMENT	17
THE CASE FOR HYBRID RF-OPTICAL COMMUNICATIONS	19
LINE OF EFFORT 1: BUILD HYBRID RF-OPTICAL NETWORKS FOR SCALE & SURVIVABILITY	19
LINE OF EFFORT 2: USE INTELLIGENT PROCESSING TO MOVE LESS DATA, FASTER	23
LINE OF EFFORT 3: OPTIMIZE & EXTEND RF PERFORMANCE	27
CHALLENGES & CONSIDERATIONS FOR IMPLEMENTATION	30
DELAYED ADOPTION CARRIES STRATEGIC RISK	30
MODERNIZATION WILL REQUIRE SUSTAINED INVESTMENT & ADAPTIVE ACQUISITION APPROACHES	30
INTEGRATING HYBRID ARCHITECTURES INCREASES OPERATIONAL & NETWORK COMPLEXITY	31
RECOMMENDATIONS & CONCLUSION	32
RECOMMENDATION 1: ACCELERATE & SUSTAIN COMMUNICATIONS MODERNIZATION THROUGH STABLE RESOURCING & ADAPTIVE ACQUISITION	32
RECOMMENDATION 2: OPERATIONALIZE HYBRID RF-OPTICAL ARCHITECTURES ACROSS THE FORCE	32
RECOMMENDATION 3: LEAD INTEROPERABILITY & STANDARDS DEVELOPMENT FOR THE FUTURE COMMUNICATIONS ECOSYSTEM	33
CONCLUSION	34

Tables & Figures

FIGURE 1: THE ELECTROMAGNETIC (EM) SPECTRUM	4
FIGURE 2: ELEMENTS OF SATELLITE COMMUNICATIONS ARCHITECTURE	5
FIGURE 3: THE SPACE ENVIRONMENT HAS CHANGED FASTER THAN MANY SUPPORTING ARCHITECTURES	6
FIGURE 4: CONVENTIONAL JAMMING/DENIAL OF SERVICE (DOS) TO USERS	7
TABLE 1: EVOLUTION OF MILITARY DECISION CYCLES	9
FIGURE 5: THE SELF-REINFORCING CYCLE	9
TABLE 2: RECENT EXAMPLES OF COMMUNICATIONS AND NAVIGATION DISRUPTION IN MODERN CONFLICT	10
FIGURE 6: GLOBAL RADIO FREQUENCY INTERFERENCE (RFI) OBSERVED BY NASA'S SMAP SATELLITE	11
FIGURE 7: RF VERSUS OPTICAL BEAM-SPREADING	12
FIGURE 8: HIGHER RESOLUTION REQUIRES HIGHER BANDWIDTH	13
TABLE 3: FROM PLATFORM-CENTRIC TO DATA-CENTRIC WARFARE	14
TABLE 4: ORBITAL REGIMES AT A GLANCE	15
TABLE 5: DRIVERS OF DATA GROWTH & RESULTING COMMUNICATIONS CHALLENGES	16
FIGURE 9: MODERN SENSING ARCHITECTURES GENERATE & DISTRIBUTE 200 TIMES MORE DATA THAN 20 YEARS AGO	16
FIGURE 10: SPACE-FARING NATIONS IN 1966 & 2020	17
TABLE 6: GROWTH OF THE GLOBAL SPACE ECOSYSTEM	18
TABLE 7: COMPETITORS ARE ALREADY INVESTING	18
FIGURE 11: NOTIONAL OPTICAL MESH NETWORK FOR SDA'S PROLIFERATED WARFIGHTER SPACE ARCHITECTURE	19
FIGURE 12: RELATIVE BEAM SPREAD OF RF & OPTICAL COMMUNICATIONS AT LONG DISTANCE	20
FIGURE 13: ILLUMA-T, LCRD, & GROUND STATIONS, DECEMBER 2023	22
TABLE 8: DATA-BURDEN REDUCTION TECHNIQUES	24
FIGURE 14: DISTRIBUTED DATA ROUTING THROUGH A SPACE-BASED MESH NETWORK	26
TABLE 9: RF TECHNIQUES: VALUABLE BUT LIMITED	28
FIGURE 15: OPTICAL COMMUNICATIONS IN MULTIPLE DOMAINS	35

Foreword

Military advantage has always depended on the ability to understand the operational environment, communicate effectively, and translate information into action faster than an adversary. Today, the ability to move, protect, process, and exploit data at speed, scale, and under attack is now a fundamental element of combat power. Modern military systems generate unprecedented volumes of data, yet much of the communications architecture upon which the military depends was designed for a less contested, less distributed, and a far less data-intensive era.

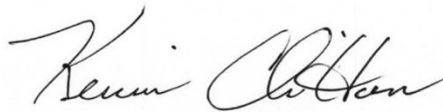
The proliferation of space-based capabilities, increasingly sophisticated sensors, distributed operations, and compressed decision timelines is imposing demands that legacy communications architectures were never designed to meet. At the same time, prospective adversaries are fielding increasingly capable means to detect, disrupt, deceive, degrade, and exploit U.S. use of the electromagnetic spectrum and associated networks. The result is not simply a technology challenge, but an operational and strategic one: whether U.S. forces can preserve the connectivity, resilience, and decision advantage required to fight effectively in highly contested environments.

In this paper, Senior Resident Fellow Jennifer Reeves argues that sustaining decision advantage will require more than incremental improvements to existing communications systems and architectures: It will require a more fundamental modernization of military information transport—one that integrates hybrid radio-frequency and optical communications, intelligent data management, and resilient, adaptive networking to provide multiple pathways for information to flow under contested conditions. These capabilities fit within the broader operational requirements for decision advantage, distributed operations, resilience, and effective combat employment—they are not isolated technical enhancements.

As the Department of Defense/War adapts for increasingly contested, distributed, and data-intensive operations, assured information movement must be treated as an operational imperative. In future conflict, the force that can maintain the integrity and flow of information while denying an adversary the same advantage will be better positioned to sense, decide, and act at the speed required to prevail. These central issues merit sustained attention from military leaders, policymakers, technologists, and industry as they shape the resilient communications and information architectures upon which America's future military effectiveness—and ultimately its ability to deter and prevail—will depend.



Lt Gen David A. Deptula, USAF (Ret.)
Dean, The Mitchell Institute for Aerospace Studies



Gen Kevin Chilton, USAF (Ret.)
Explorer Chair, MI-SPACE

Abstract

Modern warfare depends on the ability to move, integrate, protect, and exploit data at speed and scale. Existing space communications architectures, however, were designed for an earlier operational era characterized by lower data volumes, more predictable communication flows, and less contested access to space and the electromagnetic (EM) spectrum. Established radio frequency (RF) communications are now constrained by finite spectrum availability, growing bandwidth demands, and mounting vulnerability to detection, interference, jamming, and interception in contested environments. At the same time, operational timelines continue to compress, while military sensors, autonomous systems, and proliferated constellations generate unprecedented volumes of data that legacy architectures cannot efficiently transport. Communications pathways operating near capacity are harder to defend, adapt, and restore under attack or disruption. In contested environments, adversaries can exploit these limitations through jamming, cyberattacks, interception, and other forms of electronic warfare, which would degrade decision-making and operational coordination. These legacy communications architectures are increasingly unable to meet the scale, speed, and persistence of modern operational data demand. The resulting communications gap is now an operational and strategic vulnerability.

Meeting demand will require more than incremental improvements to existing networks. Hybrid RF-optical communications architectures offer a scalable path toward greater transport capacity, resilience, and survivability. Optical communications provide significantly higher throughput, reduced observability, and freedom from many of the spectrum limitations that constrain RF systems. Combined with RF's all-weather flexibility and environmental resilience, hybrid architectures can provide a more capable communications backbone for future military networks. The most practical path forward is a hybrid RF-optical communications architecture that combines RF's resilience and ubiquity with optical communications' far greater transport capacity, lower probability of intercept and detection, reduced spectrum dependence, and smaller size, weight, and power requirements.

Reducing the amount of data that must be transmitted is as important as increasing transport capacity. Onboard processing, artificial intelligence (AI), edge computing, data compression, and distributed data-management architectures can reduce transmission burdens while accelerating the delivery of mission-relevant information across operational networks. A hybrid approach, coupled with intelligent onboard data processing and continued RF modernization, can expand transport capacity, improve network resilience, and sustain U.S. decision advantage in future conflict.

The United States should accelerate the development, procurement, and fielding of hybrid RF-optical communications architectures while continuing to improve RF performance during the transition. Delayed adoption risks widening the communications gap, undermining decision advantage and ceding technological, operational, and standards-setting advantages to competitors who are already investing heavily in next-generation communications networks.

The Strategic Challenge: Legacy Communications in a Data-Intensive Battlespace

Modern warfare depends on the ability to move, integrate, protect, and exploit data across globally distributed forces operating in contested environments.¹ U.S. doctrine already recognizes the electromagnetic (EM) spectrum as a “congested, contested, and constrained” environment. This reflects the growing reality that communications are no longer simply enabling functions—they are operational targets that could collapse entire warfighting architectures.²

Communications systems are inherently vulnerable because they depend on the successful transmission and reception of precisely coordinated signals across electromagnetic pathways. Adversaries can often disrupt those transmissions through jamming, interference, cyberattacks, and signal interception. There comes a point when countermeasures can overwhelm the ability to sustain resilient communications under attack. The war in Ukraine has provided a modern demonstration of this challenge. Russian electronic warfare (EW), jamming, cyberattacks, and signal-interception operations have repeatedly disrupted Ukrainian communications, navigation, and command-and-control (C2) systems. This has degraded force coordination and reduced operational effectiveness.³ Moreover, the 2022 Russian cyberattack against ViaSat, as they were providing communications support to Ukraine, demonstrated that attacks on space-enabled communications can create cascading effects beyond the battlefield. This interrupted civilian and critical infrastructure systems: as one notable example, German wind turbines experienced impaired operational control following the attack.⁴

Legacy Architectures Were Built for a Different Era

The United States designed much of its current space communications architecture for a fundamentally different era of warfare. Until recently, access to both space and the EM spectrum was comparatively permissive, operational timelines were longer, and military decision-making followed more sequential processes. Military space systems primarily supported mission sets such as missile warning, strategic communications, and positioning, navigation, and timing. Data volumes were modest, there were fewer users, and communications were largely linear and centralized. As a result, these architectures prioritized reliability and global coverage over the scalability, flexibility, and rapid data integration demanded by today’s distributed operations.

That operational paradigm no longer holds. Modern military operations depend on rapidly integrating data from sensors, decision-makers, and weapons systems across multiple domains and echelons (see Figure 2). As operational demands have grown, legacy communications architectures designed for a smaller, slower, and more permissive space environment have become increasingly strained.

The strain is already evident. For more than a decade, elements of the Space Force’s Satellite Control Network have experienced sustained demand that exceeds industry standards. This network continues to age.⁵ Much of the architecture predates today’s proliferated space environment, with its newest major ground station completed in 1991, when fewer than 2,000 operational satellites existed worldwide (see Figure 3).⁶ Today’s communications infrastructure must support a dramatically larger and more data-intensive space enterprise than it was originally designed to sustain.

The EM Spectrum: Why It Matters

The electromagnetic spectrum encompasses a broad range of wavelengths and frequencies used for different purposes, from radio communications to visible light and X-rays. Most military satellite communications operate within the radio-frequency (RF) portion of the spectrum, a finite physical resource shared among military, commercial, and civil users. RF communications depend on access to limited portions of the electromagnetic spectrum. As the number of users, satellites, and data-intensive applications continues to grow, competition for spectrum access increases, contributing to congestion, interference, and operational constraints.

Optical communications also operate within the electromagnetic spectrum but use infrared or visible light rather than radio frequencies to transmit information. Because they rely on a different portion of the spectrum, optical links avoid many RF congestion challenges while providing significantly greater bandwidth, enabling them to complement—not replace—traditional RF communications in future hybrid architectures.

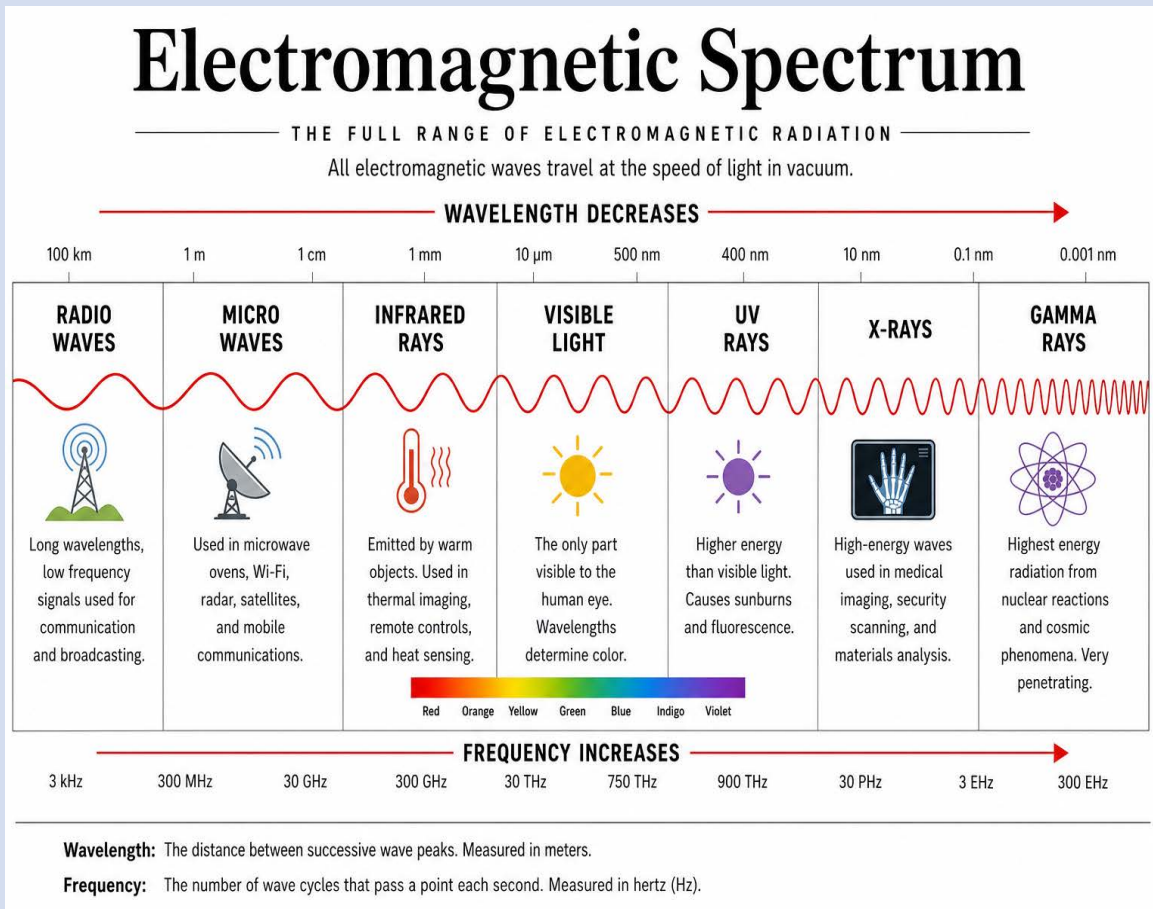


Figure 1: The electromagnetic (EM) spectrum.

Source: Mitchell Institute graphic/AI generated.

These challenges are no longer theoretical. Modern military operations require resilient, high-volume, near-real-time movement of information across globally distributed forces, yet existing communications architectures are unable to meet these increased demands. Examining the current operational environment illustrates how this communications gap has emerged and why it continues to widen.

EM&C Elements with DoD Wideband SATCOM Architecture

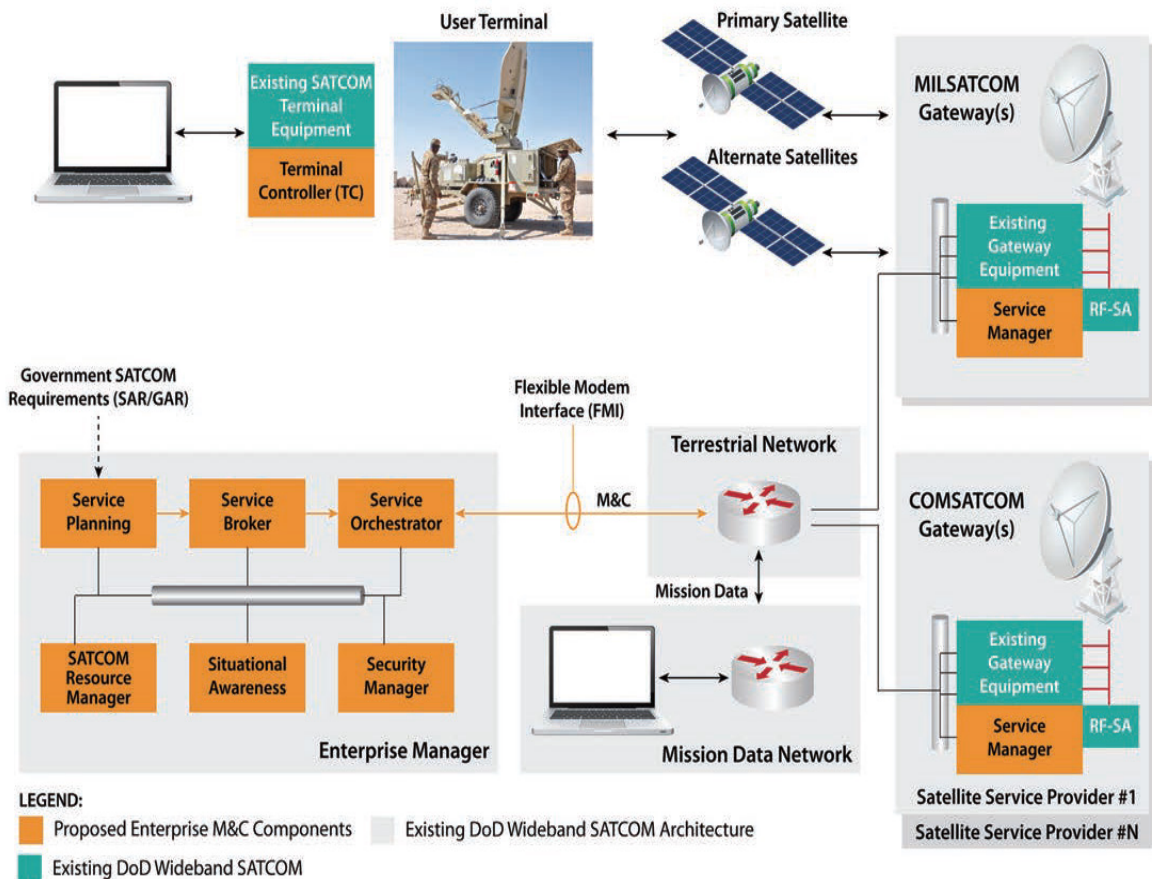


Figure 2: Elements of satellite communications architecture. Delivering data across modern military satellite communications architectures requires the successful operation of numerous interconnected systems, networks, satellites, terminals, and gateways. Disruption of any critical element can degrade overall network performance or deny communications entirely.

Source: Mark Dale, "DOD's Automated Satellite Roaming: How the Technology Protects Against Denial Of Satellite Services," Kratos Defense, March 18, 2019.

Operational Demand Is Outpacing Transport Capacity

Existing communications architectures are struggling to support the scale, speed, and persistence of modern military data flows. Emerging concepts such as distributed kill webs seek to connect globally distributed forces into resilient operational networks. These networks must be capable of detecting, processing, and acting on information faster than an adversary.⁷ U.S. forces must compress the time between detection, decision, and action to maintain operational advantage in contested environments. Yet achieving and sustaining this advantage depends on a single critical condition: the ability to transport large volumes of data quickly, securely, and reliably across the force.

Recognizing the growing operational importance of resilient, low-latency communications, the Space Force included billions of dollars for the development of its Space Data Network (SDN) in its FY 2027 budget request. The initiative seeks to integrate military, commercial, and proliferated space capabilities into a hybrid architecture capable of rapidly transferring large volumes of data across

total number of active satellites over time

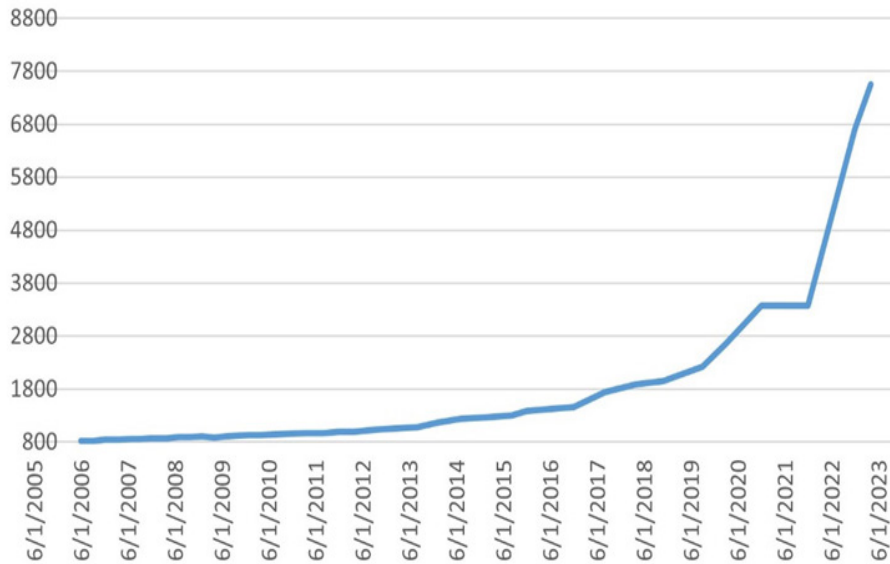


Figure 3: The space environment has changed faster than many supporting architectures. Since 2015, the number of active satellites has increased dramatically as governments and commercial providers have deployed proliferated communications, sensing, and data-transport constellations. While this growth does not directly correspond to military network demand, it illustrates the broader expansion of space activity and the data-intensive operational environment that modern communications architectures must support. As of May 31, 2026, there are 16,942 active satellites in orbit around Earth.

Source: Orbiting Now, "Active Satellite Orbit Data," accessed May 31, 2026; Laura Grego, "Our Satellite Database Reaches a Milestone. We've Learned Much Along the Way," *The Equation* blog, Union of Concerned Scientists, January 29, 2024.

domains. This investment reflects a broader operational reality: The volume and complexity of military data are increasing dramatically. Advances in sensing technologies, proliferated low-Earth orbit (LEO) constellations, and persistent missile-warning architectures are generating unprecedented volumes of information that must be collected, transported, processed, and shared across increasingly distributed networks.

This mismatch between data production and communications capacity carries direct operational consequences. Information that cannot reach commanders or weapons systems within minutes—or even seconds—may already be obsolete.⁸ Emerging threats further compress decision timelines, making latency more than an inconvenience: It becomes an operational liability. As military operations accelerate, the ability to move information rapidly determines operational effectiveness.

The communications gap also increases security risks. Because modern military operations depend on the rapid movement of information, adversaries plan to target communications through electronic warfare, jamming, cyberattacks, and signal interception. Russian operations in Ukraine have demonstrated how disrupting communications can degrade command and control and reduce operational effectiveness.⁹ Communications architectures operating near capacity are less able to reroute traffic or absorb disruptions, increasing the risk that peacetime constraints become operational vulnerabilities during conflict.

The Cost of Inaction

Information possesses a finite operational lifespan. Data that arrives after a target has moved, a decision window has closed, or an opportunity has passed may have little operational value regardless of its accuracy. As a result, communications architectures determine not only how information is shared but also which side can observe, decide, and act first. The growing communications gap therefore threatens U.S. forces' ability to maintain decision advantage in contested operations.

Twenty-first-century military operations depend on the ability to collect, move, integrate, and exploit data quickly enough to inform timely decisions. As operational timelines compress, the value of information depends on its speed of delivery and integration. Ukraine's implementation of its Delta battlefield management system—which reportedly reduced the time required to identify and engage enemy targets from 72 hours to as little as 2 minutes—illustrates the operational value of rapidly integrating and disseminating information¹⁰.

Interruptions to information flows can fragment situational awareness, delay targeting cycles, and reduce the effectiveness of integrated kill webs. Because modern military and civilian networks are interconnected, disruptions can cascade across multiple users and missions. Russia's 2022 cyberattack against the ViaSat satellite network, which supported Ukrainian operations, demonstrated how attacks on a single communications system can rapidly degrade command and control while also producing broader downstream effects.¹¹

These operational consequences extend beyond individual conflicts to shape broader strategic competition. Nations that move, protect, and exploit data more effectively will be better positioned to maintain a decision advantage and the strategic initiative in today's information-centric warfare. Maintaining U.S. leadership will therefore depend not simply on generating more data but on ensuring that critical information reaches decision-makers before opportunities disappear.

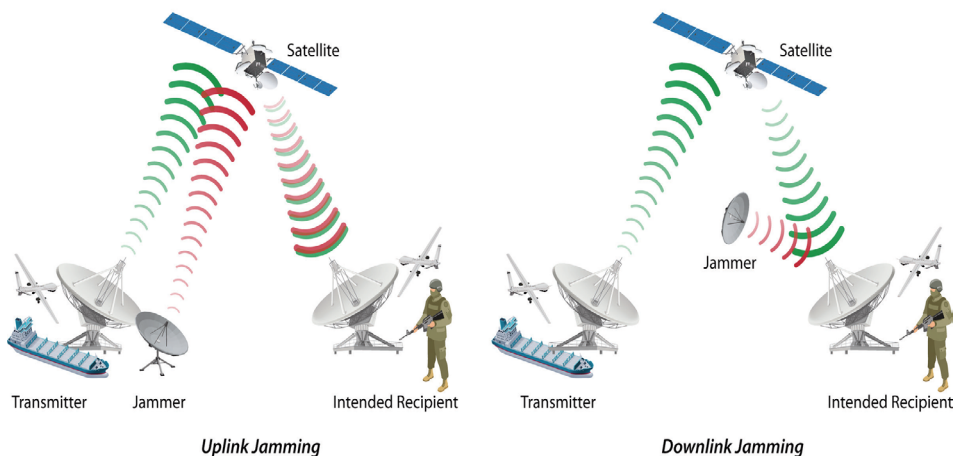


Figure 4: Conventional jamming/denial of service (DoS) to users. Successful communications require coordinated transmission, reception, timing, and routing, in addition to sufficient signal strength across the entire communications pathway. By contrast, a jammer only needs to interfere with one critical portion of the signal path to degrade or deny service. Analysts have demonstrated that portions of satellite communications traffic can be intercepted using relatively inexpensive, commercially available equipment, exposing sensitive operational information to adversaries. This asymmetry helps explain why communications systems have become attractive targets in modern warfare.

Source: Ioana Patringeraru, "The Sky is Full of Secrets: Glaring Vulnerabilities Discovered in Satellite Communications," *UC San Diego Today*, January 20, 2026; Mark Dale, "DOD's Automated Satellite Roaming: How The Technology Protects Against Denial Of Satellite Services," *Kratos Defense*, March 18, 2019.

Why Current Approaches Are No Longer Enough

Modern Warfare Depends on Decision Advantage at Speed & Scale

Modern military operations depend on the rapid movement, integration, and exploitation of data across globally distributed forces. The Department of Defense/War’s Joint All-Domain Command and Control (JADC2) concept envisions continuously connected networks linking sensors, decision-makers, and operational forces across all domains to enable faster and more informed decision-making.¹² At the same time, modern kill webs seek to connect “more sensors, across more domains, at greater distances, and at faster speeds than ever before,” making the timely movement of information essential to military effectiveness.¹³

These evolving operational concepts fundamentally change the role of communications. Rather than supporting traditional linear kill chains, communications architectures must continuously move data among distributed sensors, command elements, and weapons systems to enable “any sensor to support any shooter.”¹⁴ As operational timelines compress, delays measured in minutes—or even seconds—can determine whether information remains actionable. Communications systems are no longer simply supporting functions; they have become foundational enablers of military effectiveness itself.

As former Chief of Space Operations Gen Chance Saltzman recently noted, space capabilities are now “baked into” modern combat operations, supporting everything from global connectivity and missile warning to precision timing and distributed command and control.¹⁵ Emerging operational concepts rely on proliferated LEO architectures, hybrid cloud networks, and distributed sensing systems to maintain operations even in denied or degraded environments.¹⁶ These distributed architectures improve resilience not by preventing disruption, but by ensuring that no single attack or failure can sever the flow of operational information across the force. Military decision-making has likewise evolved from relatively linear processes to highly interconnected networks that fuse information from multiple sources in near real-time, dramatically increasing the volume, speed, and persistence of information that must be transported across military networks.

What Is a Kill Web?

Traditional military operations often rely on relatively linear kill chains in which sensors detect a target, information is passed through multiple layers of analysis and command, and weapons are ultimately employed against the target. These sequential processes can introduce delays and create vulnerabilities when individual nodes are disrupted.

A kill web seeks to create a more resilient and adaptable architecture by connecting multiple sensors, decision-makers, and weapons systems across domains. Rather than relying on a single pathway, information can move through multiple routes, enabling forces to identify targets, coordinate effects, and respond more rapidly in contested environments. The effectiveness of a kill web depends on its ability to move, integrate, protect, and exploit information across the network. Communications disruptions, latency, or data bottlenecks can therefore degrade the speed and effectiveness of the entire system.

Adapted from Heather R. Penney, *Scale, Scope, Speed & Survivability: Winning the Kill Chain Competition*

Traditional Warfare	Modern Warfare
Sensor	Sensor Network
↓	↓
Observe	Data Fusion
↓	↓
Orient	AI-Assisted Orientation
↓	↓
Decide	Decision Support
↓	↓
Act	Action
Hours → Days	Seconds → Minutes

Table 1: Evolution of military decision cycles.

These trends reinforce one another. As military organizations deploy more sensors, they generate greater volumes of information requiring transport, processing, and dissemination. At the same time, commanders become increasingly dependent on rapidly integrating that information to support operations. Each additional sensor improves resilience and situational awareness while simultaneously increasing network traffic. This creates a cycle in which both data generation and data consumption accelerate. The result is a steadily growing demand for communications architectures capable of moving information rapidly across globally distributed forces (see Figure 5).

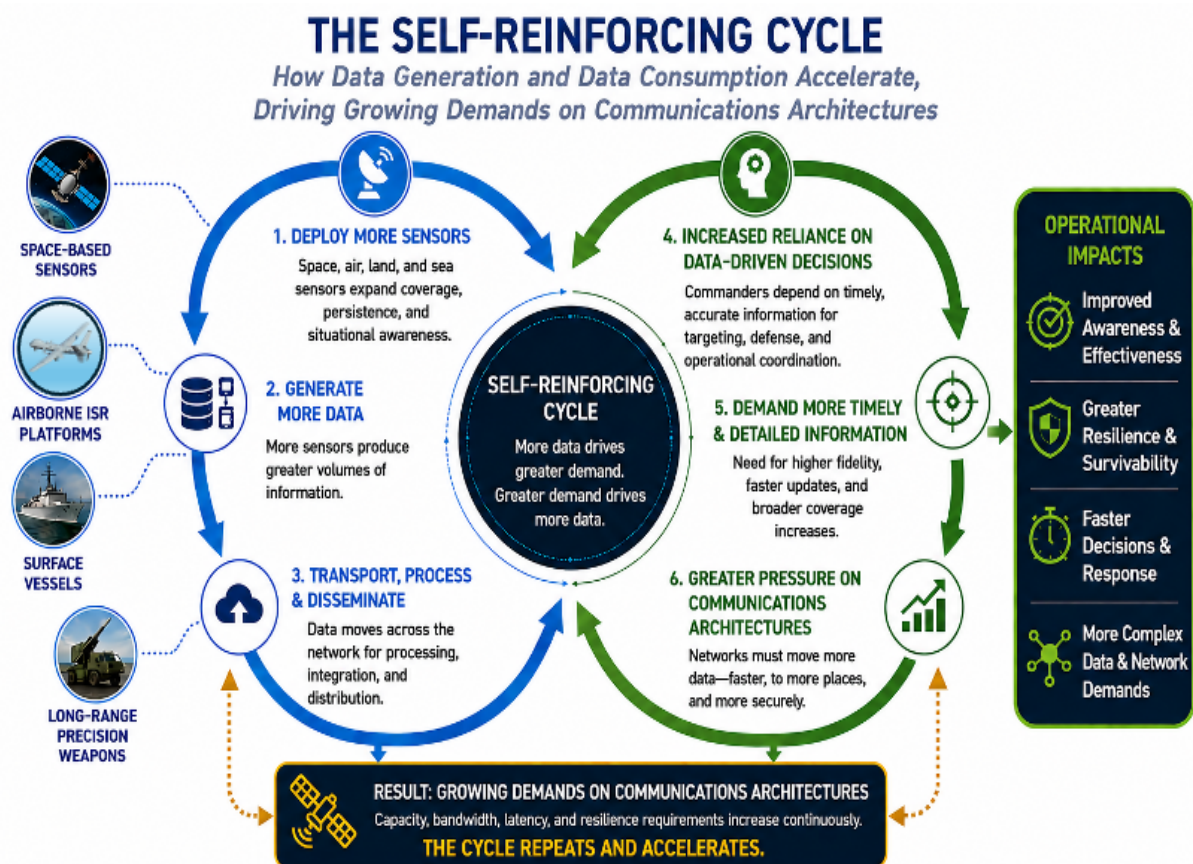


Figure 5: The self-reinforcing cycle.

Source: Mitchell Institute graphic/AI generated.

Contested Environments Are Hostile to Legacy Communications

RF communications operate in an inherently observable and contested EM environment where every transmission can serve as a detectable target. Unlike wired or physically isolated communications pathways, RF transmissions propagate openly through the atmosphere and orbital environment. The transmissions are thus exposed to detection, interception, geolocation, interference, and exploitation by both friendly and adversarial actors. This makes the signals themselves observable, targetable, and exploitable by friend and foe alike. These characteristics are not temporary technical shortcomings but inherent properties of RF transmission itself.

The Space Force's Future Operating Environment projects that future conflicts will treat the EM spectrum as contested terrain, where competition extends beyond platforms to the signals themselves. Although that assessment looks toward 2040, recent operations already demonstrate that electronic attack, spectrum denial, and signal exploitation have become routine features of modern warfare.¹⁷ As a result, communications architectures designed around continuous connectivity, centralized control, and uninterrupted access to the EM spectrum—like the United States' legacy communications architectures—become increasingly vulnerable in contested operational environments. This operational reality is reflected in doctrine, real-world operations, and measurable impacts from disruption. Various government policies already characterize the EM spectrum as a “congested, contested, and constrained” environment, acknowledging that spectrum access can no longer be assumed during modern military operations.¹⁸ Recent battlefield experience illustrates this reality (see Figure 6).

Ukraine serves as a modern case study demonstrating how military forces heavily dependent on the RF spectrum for communications, navigation, and command and control are vulnerable to electronic warfare, jamming, interception, and self-induced disruption.¹⁹ Russian electronic warfare activities in Ukraine have repeatedly degraded drone operations, communications, and battlefield coordination, while GPS interference in the Baltic region has disrupted aviation, navigation, and flight operations.²⁰

Event	Method	Operational Effect	Strategic Lesson
ViaSat KA-SAT (2022)	Cyberattack	Disrupted satellite communications across Ukraine and Europe	Space-enabled services are vulnerable to non-kinetic attack
Ukraine Conflict (2022–ongoing)	Electronic warfare and jamming	Degraded drone operations, communications, and battlefield coordination	Information superiority is contested
Baltic Region GPS Interference (ongoing)	GNSS jamming	Disrupted aviation navigation and flight operations	Positioning, Navigation & Timing disruption affects military and civilian users
Red Sea Maritime Operations (ongoing)	GPS spoofing	Affected ship navigation and maritime situational awareness	Navigation data can be manipulated, not merely denied

Table 2: Recent examples of communications and navigation disruption in modern conflict.

Source: Victoria Samson, “[Global Counterspace Capabilities 2026](#),” Secure World Foundation, April 2026.

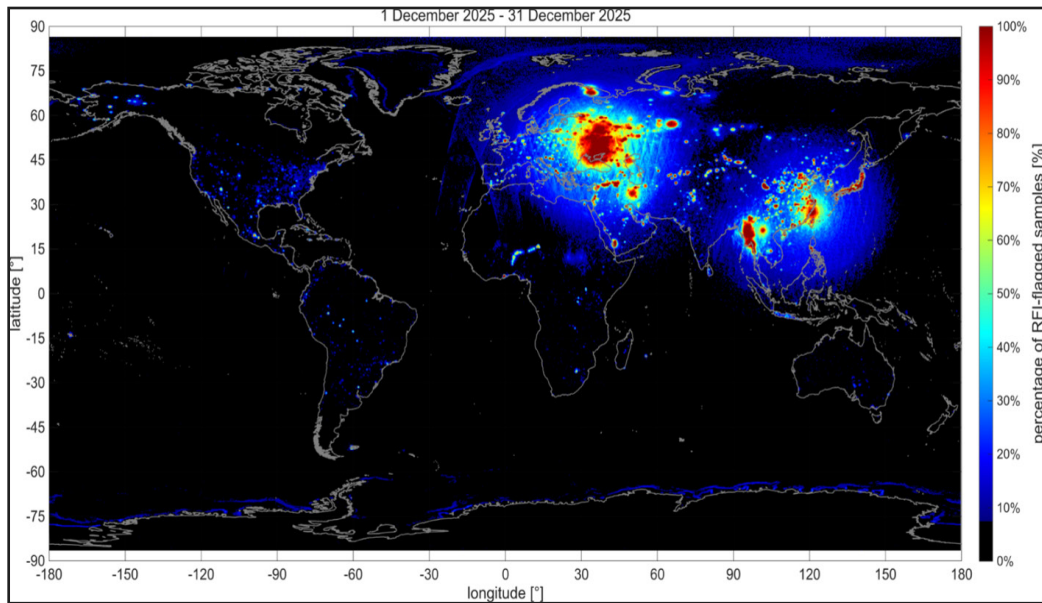


Figure 6: Global radio frequency interference (RFI) observed by NASA's SMAP satellite. Areas of persistent radio frequency interference (RFI) are concentrated in regions with heavy spectrum utilization and population density, illustrating the growing congestion of the electromagnetic environment. As demand for spectrum access continues to increase, available bandwidth becomes more constrained, reducing operational flexibility and rising susceptibility to interference.

Source: NASA Goddard Space Flight Center. Monthly RFI map derived from observations by the [Soil Moisture Active Passive \(SMAP\) satellite](#).

Resilient communications become increasingly difficult and costly because adversaries actively exploit the electromagnetic spectrum to shape operational outcomes. Electronic warfare, jamming, spoofing, cyberattacks, and signals interception are no longer supporting activities; they have become integral components of modern military campaigns. Assuming military forces only become more dependent on distributed operations, networked command and control, and rapid data exchange, disruptions to those communications pathways become an appealing approach for adversaries to degrade coordination, slow decision-making, and reduce operational effectiveness across multiple domains simultaneously.²¹

At the same time, as the joint force becomes more dependent on globally integrated, data-intensive operations, the vulnerable RF pathways and potential attack surfaces will expand in both number and extent. Disruptions that once would have affected only isolated systems now risk cascading across interconnected operational networks supporting command and control, targeting, navigation, sensing, logistics, and distributed decision-making. As a result, RF-dependent architectures risk degraded operational coordination, slower decision-making timelines, fragmented distributed operations, and reduced resilience and effectiveness of globally integrated military activities. To address the vulnerabilities exposed by dependence on RF links, the Department of Defense/War must evolve to a hybrid approach that leverages the physical and informational advantages of optical communications.

Unlike traditional RF transmissions, whose energy spreads over distance even when transmitted through directional antennas, optical communications concentrate energy into extremely narrow beams that remain tightly focused over long distances (see Figure 7). This highly directional propagation reduces the probability of

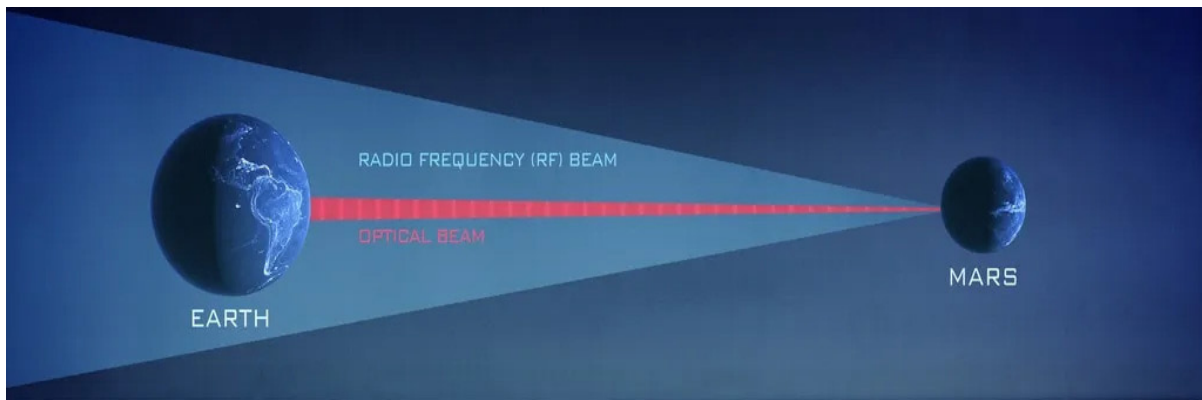


Figure 7: RF versus optical beam-spreading. Like the difference between the broad illumination of a flashlight and the tightly focused beam of a laser pointer, RF transmissions spread over much larger areas than optical beams, increasing the likelihood of detection and interception.

Source: Graphic by Katherine Schauer, "Laser Communications: Empowering More Data Than Ever Before," NASA/Goddard Space Flight Center, May 12, 2021.

detection, interception, geolocation, and interference. It also enables substantially greater data transport capacity. In operational terms, optical communications provide a more discrete and resilient transport pathway for moving large volumes of mission-critical data between satellites, ground nodes, and operational forces. Although optical systems introduce their own technical and environmental challenges, particularly for atmospheric transmission, their reduced observability and high throughput make optical links an operational imperative to function in contested environments.²² Although optical communications address many of the capacity and survivability limitations of legacy RF systems, they are intended to complement—not replace—RF communications. Future military networks will rely on hybrid architectures that combine the strengths of both technologies, making continued improvements in RF performance as important as advances in optical communications.

While hybrid and optical architectures offer longer-term pathways toward more survivable communications transport, greater RF agility and transmission resilience can achieve more immediate improvements. Modern anti-jam and spread-spectrum techniques are specifically designed to make RF signals more difficult to detect, target, disrupt, and exploit within contested electromagnetic environments. Rather than relying on fixed frequencies or static transmission methods, these approaches dynamically adapt how signals are transmitted across the spectrum to complicate adversary interference and improve survivability during contested operations. Spread-spectrum waveforms, for example, distribute transmissions across a broad range of frequencies, forcing a jammer either to expend significantly more power or to attempt to disrupt a much larger portion of the spectrum to achieve meaningful effects. Approaches such as this improve the flexibility, survivability, and resilience of RF communications operating within congested and contested environments. They do not eliminate the observable nature of the electromagnetic spectrum, nor can they make RF transmissions fully private or invulnerable. What they can do is make it substantially more difficult for adversaries to exploit the inherent vulnerabilities of RF-based communications architectures.

RF-based communications systems' vulnerabilities are emerging at the same time that proliferated sensing systems, distributed operations, and persistent global connectivity are dramatically increasing the volume of data that military communications architectures must transport. As modern operations become both more connected and more data-intensive, existing communications systems face growing pressure not only from adversaries, but also from the sheer scale and complexity of operational data demand.

Data Production Is Rising Faster Than Legacy Networks Can Absorb

Emerging operational concepts such as Joint All-Domain Command and Control (JADC2) envision continuously connected networks linking sensors, decision-makers, and operational forces across multiple domains in near real-time.²³ Moreover, distributed operations, proliferated sensing architectures, persistent global surveillance, and compressed decision timelines are collectively transforming military effectiveness into a fundamentally data-centric challenge (see Figure 8). In this environment, operational success depends on rapidly and reliably transporting large volumes of data across highly interconnected networks that support multiple functions. These include command and control, targeting, navigation, sensing, logistics, and distributed decision-making, to name a few.²⁴ Yet many existing communications architectures were designed for a fundamentally different operational paradigm.

Why Modern Sensors Generate More Data

Improvements in sensor resolution dramatically increase the amount of information collected during each observation. Higher-resolution imagery captures more detail, supports more precise analysis, and enables new operational applications. Still, it also generates substantially larger data volumes that must be transmitted, processed, stored, and exploited. As sensing technologies continue to advance, the growth in data demand reflects not only more observations but also information-rich observations. Modern sensing architectures therefore increase demand in both directions—they collect substantially more data more frequently during each collection event.

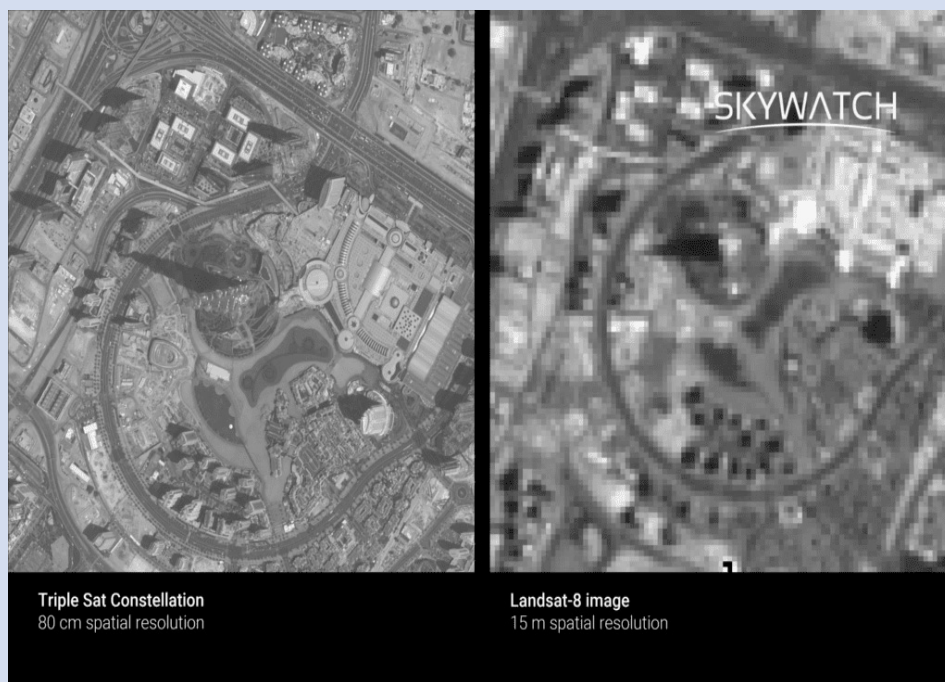


Figure 8: Higher resolution requires higher bandwidth.

Credit: Side-by-side comparison of the Burj Khalifa in Dubai, imaged by the Triple Sat Constellation at 30-centimeters spatial resolution and by Landsat-8 at 15-meter spatial resolution. Skywatch, [“What resolution do I need when using satellite data?”](#) July 11, 2022.

One of the largest drivers of surging data production and transportation is the explosive growth in the number of satellites orbiting Earth. Proliferated satellite constellations are major contributors to the dramatic increase in systems simultaneously generating, transmitting, and routing operational data across military and commercial space networks. Unlike earlier space architectures that relied on relatively small numbers of highly capable satellites operating through largely centralized communications pathways, modern proliferated LEO architectures distribute sensing, communications, and networking functions across a large number of interconnected platforms. As proliferated constellations continue to expand, communications architectures must support global data flows originating from a growing number of interconnected systems operating in parallel. Rather than episodic communications between a more limited number of platforms, modern architectures require the persistent movement of information across globally distributed constellations that support missile warning, tactical communications, space domain awareness, environmental sensing, targeting support, and distributed command and control (see Table 3).²⁵

This growth is driven not only by increasing data demand, but also by the practical realities of orbital mechanics. Unlike GEO systems, proliferated LEO constellations require a substantially larger number of satellites to achieve continuous global coverage. As a result, modern architectures rely on hundreds of interconnected spacecraft rather than a handful of geostationary platforms, dramatically increasing the number of systems simultaneously generating and exchanging operational data (see Table 4). The Space Development Agency’s (SDA) transport layer, for example, is forecasted to have more than 100 satellites in LEO by 2027.²⁶

Advanced sensing systems are dramatically increasing both the volume and complexity of operational data moving across military and commercial space networks. Modern proliferated constellations operated by government and commercial providers generate continuous streams of data through high revisit rates and diverse

Historical Environment	Current Environment
Hundreds to low-thousands of satellites	More than 15,000 active satellites worldwide
Episodic collection and scheduled observations	Persistent monitoring and continuous sensing
Single-purpose satellite missions	Multi-mission and multi-sensor architectures
Lower-resolution imagery and limited data products	High-resolution, multispectral, and hyperspectral data products
Data measured primarily in gigabytes (GB: 1 billion bytes)	Data increasingly measured in terabytes (TB: 1 trillion bytes) and petabytes (PB: 1 quadrillion bytes)
Sequential command-and-control processes	JADC2-enabled, data-driven kill webs
Decision cycles measured in hours or days	Decision cycles increasingly measured in minutes or seconds

Table 3: From platform-centric to data-centric warfare. The cumulative effect of these changes is a dramatic increase in the volume, velocity, and complexity of information that military communications architectures must transport.

Why Hyperspectral Imaging Generates So Much Data

Traditional imaging systems capture only a handful of visible color bands, such as red, green, and blue. Hyperspectral sensors, by contrast, collect data across hundreds of narrow spectral bands spanning visible and infrared wavelengths, creating a detailed “spectral fingerprint” for every pixel in an image. This enables analysts to distinguish materials that appear identical to the human eye. For example, it can differentiate healthy from stressed vegetation, identify disturbed soil, detect camouflage, or recognize specific minerals and man-made materials. The tradeoff is data volume: A single hyperspectral image can contain hundreds of times more information than a comparable conventional color image, creating significant storage, processing, and communications demands. As hyperspectral sensing becomes more common in military and commercial space systems, onboard processing and intelligent filtering become more important to ensuring that only mission-relevant information—not every raw pixel—is transmitted over constrained communications networks.

sensing modalities. These datasets consist of optical and synthetic aperture radar (SAR) high-resolution imagery, tracking data, environmental sensing, missile warning, and space domain awareness information.²⁷ At the same time, sophisticated sensors are producing dramatically larger datasets: A single high-resolution satellite image, for example, can exceed 2 GB. Many of these data products require significant processing before they can support operational decision-making. Analysis from the National Academies of Sciences notes that improvements in sensor resolution, persistence, and revisit rates have driven a 200-fold increase in data output over the last 20 years, placing significant strain on communications architectures already operating near capacity (see Figure 9).²⁸ Modern communications systems must transport not only more data, but richer, more time-sensitive, and more computationally demanding information across increasingly interconnected military and commercial networks (see Table 5).

Existing RF-based communications architectures already struggle to absorb this growing demand because they operate within a finite, heavily regulated, and shared electromagnetic spectrum.²⁹ Unlike computing power or data storage, usable spectrum cannot simply be expanded to match demand. As proliferated constellations, advanced sensing systems, commercial networks, and military operations continue to grow simultaneously, increasing volumes of data must compete for limited transmission opportunities, forcing tradeoffs. The challenge is therefore not merely technological, but structural. Spectrum availability, transmission power limitations, orbital coordination requirements, and shared access constraints collectively impose hard ceilings on overall transport capacity.

Orbit	Approximate Altitude	Key Characteristics	Typical Uses
Low Earth Orbit (LEO)	160–2,000 km	Closest to Earth; low latency; requires large constellations for continuous global coverage because satellites move rapidly across the sky	Communications, Earth observation, missile warning, space domain awareness, proliferated constellations (e.g., Starlink, SDA Proliferated Warfighting Space Architecture)
Medium Earth Orbit (MEO)	2,000–35,786 km	Covers larger geographic areas than LEO with fewer satellites; moderate latency and longer orbital periods	Positioning, Navigation, and Timing (PNT) services such as GPS, Galileo, and other navigation constellations
Geosynchronous Earth Orbit (GEO)	35,786 km	Satellites orbit at the same rate that Earth rotates, appearing fixed over a single location; provides persistent regional coverage but with higher latency	Strategic communications, missile warning, weather monitoring, and national security missions requiring continuous coverage

Table 4: Orbital regimes at a glance.

Driver of Data Growth	Why It Increases Data Volume	Communications Impact
Proliferated LEO constellations	Thousands of additional collection and relay nodes continuously generate and exchange data	Increases demand for transport capacity across the network
Higher-resolution sensors	More pixels, spectral bands, and precision create significantly larger files	Requires greater bandwidth and longer transmission times
Persistent monitoring	Continuous observation generates data streams rather than periodic snapshots	Reduces opportunities to clear transmission backlogs
Multi-sensor payloads	Satellites increasingly collect imagery, RF, weather, navigation, and other data simultaneously	Increases the volume and complexity of data requiring transport
Time-sensitive operations	JADC2, missile warning, and kill-web operations require rapid dissemination and exploitation	Reduces tolerance for latency and communications bottlenecks

Table 5: Drivers of data growth & resulting communications challenges.

As demand increases, operators are forced to make tradeoffs in how information is transmitted, prioritized, and delivered across the network. In practice, this may require prioritizing missile-warning and command-and-control traffic over other lower-priority products. This might mean delaying imagery transmission, compressing data files, or accepting greater latency in less time-sensitive applications.³⁰ These pressures are compounded by finite downlink opportunities, crowded transmission pathways, and the burden associated with coordinating large numbers of interconnected systems simultaneously exchanging mission-critical information. While incremental improvements such as adaptive waveforms, spectrum sharing, and more efficient RF management can extend system performance, they cannot eliminate the underlying mismatch between rapidly growing data production and finite transport capacity.³¹

Total Data Volume and Data Files Distributed by Year

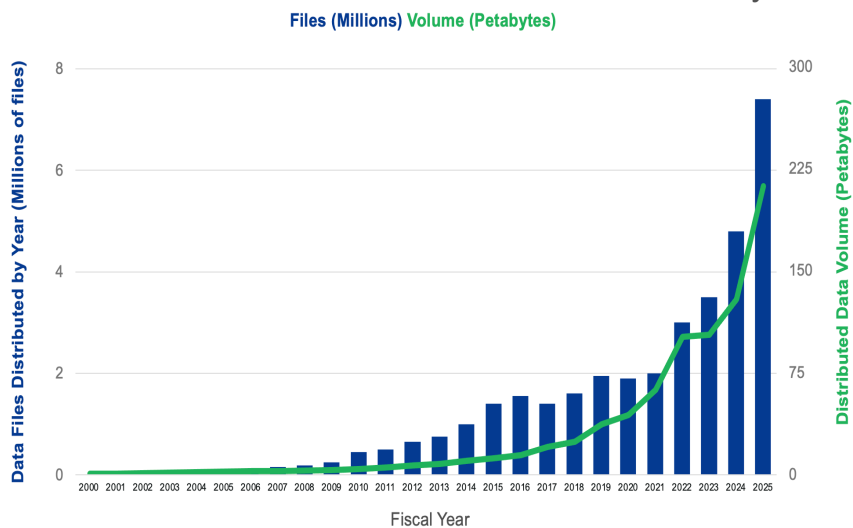


Figure 9: Modern sensing architectures generate & distribute 200 times more data than 20 years ago. NASA Earthdata metrics illustrate the rapid growth in archived and distributed Earth-observation data enabled by persistent sensing systems, proliferated collection architectures, and sophisticated space-based sensors. The scale and persistence of modern data generation are placing growing demands on communications architectures responsible for transporting, processing, and disseminating information globally

Credit: "Earth Science Data Systems 2025 Fiscal Year Highlights," accessed July 1, 2026.

The result is a growing communications gap in which the joint force's ability to collect data is rapidly outpacing its ability to transport, process, and operationally exploit it. As proliferated constellations, advanced sensing systems, and globally integrated operations continue to expand, this imbalance risks slowing decision-making, fragmenting distributed operations, and eroding decision advantage across the force. Communications capacity is emerging as a limiting factor in the joint force's data usage. Unaddressed, this communications gap threatens to undermine the United States' current operational advantage and global dominance.

Strategic Competition Is Shaping the Future Communications Environment

Space communications are rapidly becoming a central arena of strategic competition. The ability to move, protect, process, and exploit data at scale will shape future military effectiveness, alliance integration, commercial influence, and crisis response. As warfare becomes ever more data-centric, communications architectures will determine how rapidly nations can integrate information, coordinate operations, and maintain a decision advantage. Leadership in communications architecture is therefore becoming closely tied to broader geopolitical and military influence.³²

The United States' strategic competitors are actively investing in next-generation communications systems designed around scale, resilience, and advanced data transport capabilities. Analyses from the Secure World Foundation and the U.S. Space Force highlight that nations such as China are rapidly developing proliferated constellations, advanced networking systems, and space architectures intended to support their own data-intensive military operations.³³ Furthermore, reporting on China's growing laser communications sector indicates significant investment in optical networking and satellite communications technologies capable of supporting high-capacity and resilient space-based data transport.³⁴ Other nations, including India, are also expanding their own space communications and data-relay capabilities as part of broader efforts to strengthen indigenous space architectures and operational autonomy (see Table 7). The future communications environment is already being shaped by global competition over data transport, networking, and resilient space infrastructure. The United States must not fall behind.

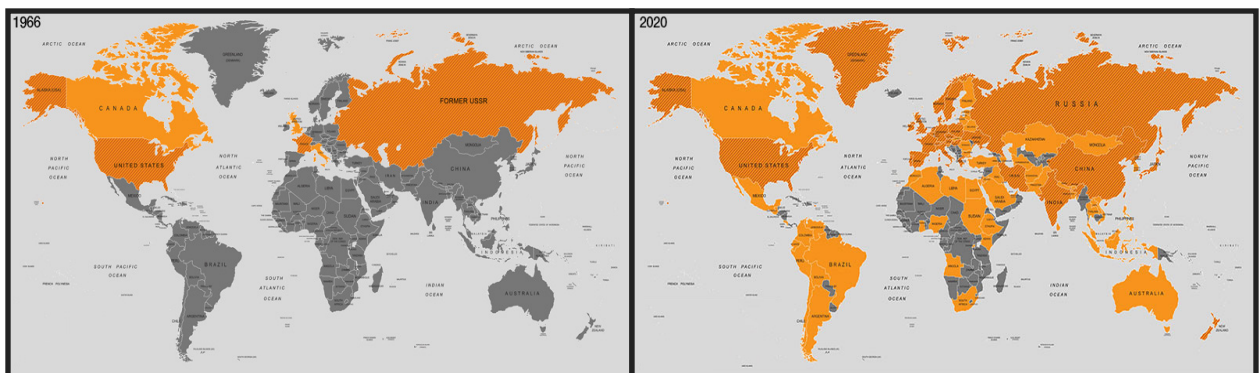


Figure 10: Space-faring nations in 1966 & 2020. The global space ecosystem has expanded dramatically over the past six decades. More nations now possess launch capabilities and operate satellites, increasing international competition while accelerating demand for resilient communications, networking, and data-transport architecture. Light orange countries have assets in space; dark orange countries have launch capabilities in addition to assets in space.

Credit: "[Union of Concerned Scientists Satellite Database](#)," Union of Concerned Scientists, published December 8, 2005, updated May 1, 2023.

	Nations with orbital-launch capability	Annual launches	Nations with satellites/payloads in orbit	Active satellites
1980	7	108	18	~400
1990	8	114	29	~500
2000	8	81	46	~800
2010	9	70	59	~1,000
2020	13	104	100	~2,500
2025	13	315	116	~15,000

Table 6: Growth of the global space ecosystem. The rapid expansion of launch activity, participating nations, and active satellites illustrates the accelerating growth of the global space ecosystem and the corresponding demand for resilient communications and networking architectures.

Credit: Data from Jonathan McDowell, "[Jonathan's Space Pages](#)," accessed July 1, 2026.

	Example Initiative	Strategic Significance
China	Optical communications demonstrations and mega-constellations	Shapes future architectures and standards
Europe	HydRON optical networking initiative	Develops sovereign communications capabilities
India	Laser communications and relay network investments	Expands independent space networking capacity
Japan	Optical communications demonstrations	Advances next-generation communications technologies
United States	SDA Transport Layer and commercial optical meshes	Maintains leadership through government-commercial integration

Table 7: Competitors are already investing.

The strategic implications extend beyond simply fielding faster communications systems. Nations that move early to adopt emerging architectures will gain disproportionate influence over the standards, interoperability frameworks, operational concepts, and integration pathways that define future systems.³⁵ The 5G experience offers a useful cautionary example by illustrating why early participation in standards development matters. China's early and coordinated push into 5G, spectrum policy, and international standards bodies gave it significant influence over the technical and commercial environment in which future networks would operate.³⁶ Although the United States remained a leader in telecommunications innovation, it was often forced to compete within portions of a standards ecosystem it had not primarily shaped.³⁷ In the space communications sector, similar dynamics will shape optical terminal interfaces, crosslink standards, spectrum coordination, data-relay architectures, and allied interoperability. Failure to lead, therefore, risks more than a technological disadvantage. It risks forcing the United States to operate within communications architectures and operational assumptions influenced by competitors.

The communications gap facing the United States is an operational and strategic challenge at the intersection of data growth, contested RF environments, proliferated space architectures, and intensifying global competition, not merely a technical shortfall inside existing systems.

Legacy space communications architectures are not merely strained—they are misaligned with the requirements of modern warfare. Incremental improvements to legacy RF networks will not be enough. Preserving decision advantage will require a different approach to moving, processing, and protecting information at operational speed and scale. The question, then, is not whether change is necessary, but which combination of technologies and concepts offers the most practical path forward.

The Case for Hybrid RF-Optical Communications

Addressing the U.S. communications gap requires a layered approach that expands communications capacity through hybrid RF-optical architectures, reduces transmission burdens through intelligent processing, and improves the resilience and efficiency of existing RF systems as the enterprise moves toward next-generation architectures. Because the communications gap results from multiple reinforcing pressures on modern military networks—including transport bottlenecks, escalating data demands, and growing vulnerabilities in contested electromagnetic environments—solving this problem requires similarly interrelated, reinforcing efforts. No single technology can resolve the growing communications gap. The solution must comprise a multi-level approach that simultaneously expands transport capacity, reduces transmission burdens, and improves the resilience of existing communications pathways. Together, these efforts provide a practical roadmap for sustaining decision advantage in a data-intensive battlespace.

Line of Effort 1: Build Hybrid RF-Optical Networks for Scale & Survivability

Optical communications expand transport capacity beyond RF limitations. Optical communications operate at frequencies measured in hundreds of terahertz, far beyond the comparatively narrow gigahertz frequencies used by traditional RF systems. These frequencies dramatically increase the amount of data that can be transmitted within a single pathway.³⁸ Laser communications will be a “step-change” improvement in transport capacity compared to traditional RF systems, particularly for space-to-space applications where atmospheric interference is absent.³⁹

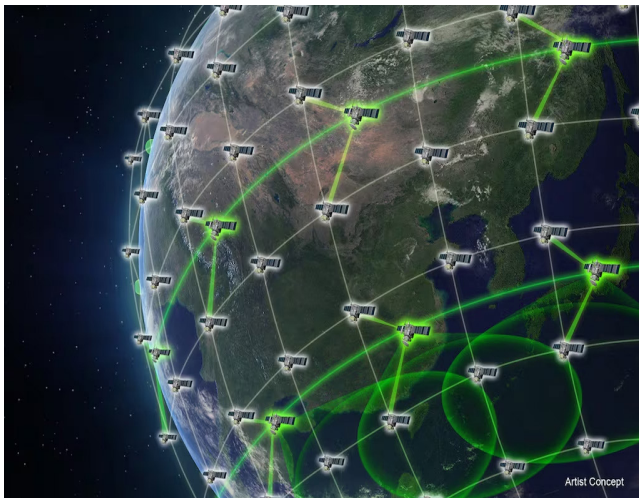


Figure 11: Notional optical mesh network for SDA's Proliferated Warfighter Space Architecture. Optical inter-satellite links enable data to move directly across a proliferated constellation rather than relying solely on terrestrial relay infrastructure. By creating multiple pathways for information flow, optical mesh networks improve resilience, reduce latency, and support the rapid movement of mission-critical data across globally distributed military operations.

Credit: [DARPA](#).

Amazon's Project Kuiper has demonstrated optical inter-satellite data transmission at rates of 100 gigabit per second over distances of approximately 1,000 kilometers, proving the ability to dynamically move large volumes of data across a distributed satellite mesh network without relying on immediate ground relays.⁴⁰ Government and defense programs are similarly demonstrating operational maturity. In 2025, General Atomics Electromagnetic Systems successfully demonstrated an interoperable air-to-space optical communications link using an SDA-compatible optical terminal and a commercial satellite, validating multi-vendor laser communications architectures that support the Proliferated Warfighter Space Architecture.⁴¹ Unlike traditional communications architectures that often depend on routing data through a limited

number of ground stations and congested RF pathways, optical crosslinks allow information to move directly between satellites across a proliferated constellation. Data can thus be rerouted around degraded nodes, transmitted across regions lacking ground infrastructure, and delivered with significantly lower latency times across globally distributed networks. As proliferated military constellations continue to expand, these capabilities are becoming more important for transporting time-sensitive operational data—including missile tracking, targeting, and battlespace awareness information.

Why Optical Communications Are Different

Optical communications are not intended to replace RF. Instead, they complement existing RF networks by providing high-capacity, low-probability-of-intercept/low-probability-of-detection transport links. At the same time, RF continues to provide broad-area coverage, broadcast services, and communications in degraded weather conditions. Together, hybrid RF-optical architectures combine the strengths of both technologies to create more resilient military communications networks.

Characteristic	Radio Frequency (RF)	Optical (Laser)
Bandwidth	Limited spectrum availability	Vast optical spectrum enables much higher data rates
Beam width	Broad transmissions	Extremely narrow, highly focused beams
Detection & interception	Easier to detect, intercept, and geolocate	Lower probability of detection and interception
Terminal size	Larger antennas/apertures	Smaller optical apertures reduce size, weight, and power requirements
Spectrum congestion	Increasingly crowded	Operates outside congested RF bands
Atmospheric effects	Generally resilient	Clouds and atmospheric turbulence affect space-to-ground links; space-to-space links are largely unaffected

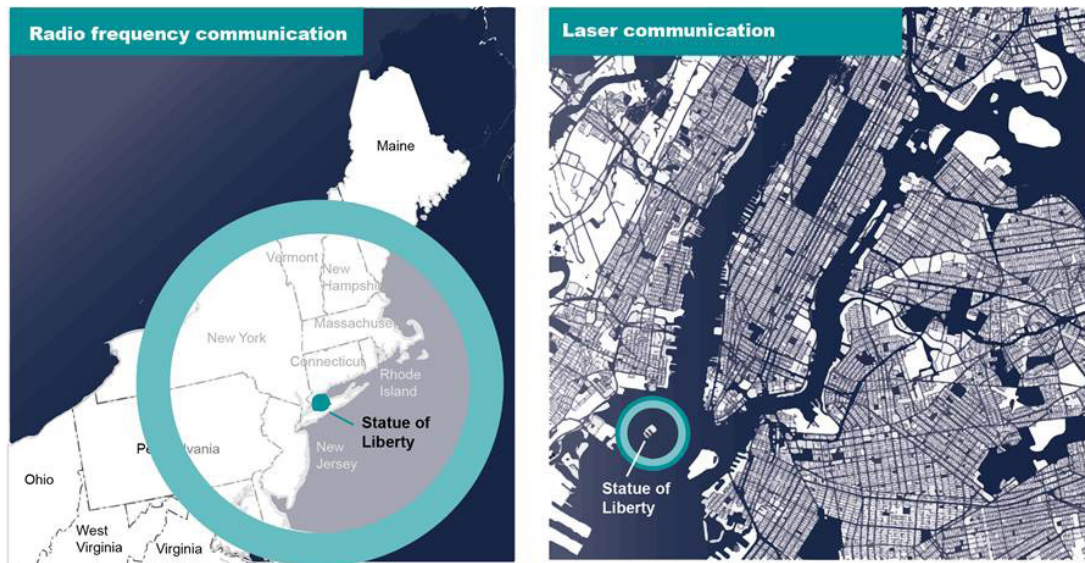


Figure 12: Relative beam spread of RF & optical communications at long distance. From low Earth orbit, radio frequency transmissions spread across a much larger area on the ground than tightly focused optical communications. The narrower optical beam concentrates energy and data within a much smaller footprint, reducing opportunities for detection, interception, and interference while supporting higher-capacity data transmission.

Credit: GAO.

Furthermore, optical communications enable fundamentally different network architectures than traditional RF-dependent systems. Optical crosslinks facilitate satellites to transfer data directly across proliferated constellations through persistent mesh-style networks. Rather than routing information through terrestrial infrastructure for redistribution (as traditional RF networks primarily do), optical networks dynamically move data across multiple satellites until it reaches the most effective downlink station or operational user. This reduces dependence on fixed ground infrastructure while improving resilience, routing flexibility, and continuity of operations across globally distributed theaters.

SDA identified optical inter-satellite links as a foundational component of its future transport architecture as early as 2020, emphasizing their role in enabling resilient, beyond-line-of-sight data movement supporting missile tracking, targeting, and distributed C2 operations.⁴² This early investment reflects a broader recognition that proliferated constellations require the persistent movement of time-sensitive data across large numbers of interconnected systems. As military networks continue shifting toward distributed operations and globally integrated kill webs, optical mesh networking provides the scalable transport layer needed to move operational data rapidly across geographically dispersed forces, sensors, and decision-makers, even in degraded or contested environments (see Figure 11).

Highly directional optical links improve survivability and scalability. Optical communications offer significant survivability advantages in contested electromagnetic environments. They concentrate energy into extremely narrow beams, making transmissions substantially more difficult to detect, intercept, geolocate, or jam than traditional RF signals. The Government Accountability Office (GAO) similarly concludes that tightly directed optical transmissions reduce susceptibility to interception while minimizing interference between systems. Unlike RF communications, which compete for access within a finite and congested spectrum, optical systems operate outside traditional spectrum constraints and generally require smaller, lighter, and less power-intensive terminals. Together, these characteristics improve the survivability, scalability, and operational resilience of distributed military communications architectures.⁴³

Hybrid RF-optical architectures combine scalability, flexibility, and redundancy. Future military space architectures should employ hybrid RF-optical architectures to combine the strengths of both approaches: RF provides broad-area coverage and all-weather communications, while optical links offer higher throughput, lower probability of intercept, and more efficient movement of large data volumes across distributed networks. Rather than replacing RF systems outright, optical communications are emerging as a complementary transport layer that can relieve pressure on congested RF pathways and improve overall network resilience and scalability.

NASA's Laser Communications Relay Demonstration (LCRD) and Integrated Laser Communications Relay Demonstration Low Earth Orbit User Modem and Amplifier Terminal (ILLUMA-T) provide an operational example of this hybrid approach (see Figure 13). The systems demonstrated two-way optical relay communications at data transmission rates approaching 1.2 gigabits per second by integrating optical transport capabilities into broader communications networks. These demonstrations reflect a growing recognition that future architectures will require multiple complementary transport layers to balance capacity, resilience, latency, and environmental constraints across global operations.⁴⁴

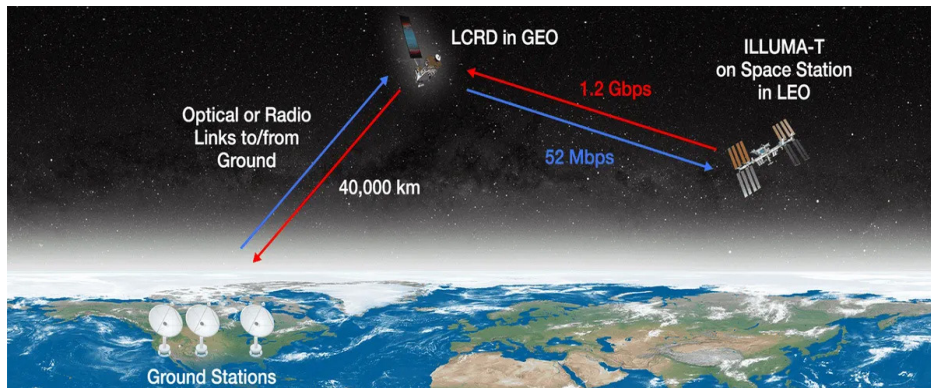


Figure 13: ILLUMA-T, LCRD, & ground stations, December 2023. NASA's LCRD and ILLUMA-T demonstrated operational two-way laser communications linking LEO, GEO, and ground stations. The program validated a key building block for future hybrid RF-optical communications architectures capable of transporting large volumes of data across distributed space networks.

Image credit: [NASA](#).

Government and industry demonstrations validate growing operational maturity. Optical communications are rapidly transitioning from experimental demonstrations to operationally relevant capabilities. Advances in pointing, acquisition, and tracking technologies have overcome many of the technical challenges that historically limited the adoption of optical communications.⁴⁵ Furthermore, recent government demonstrations—including NASA's LCRD, ILLUMA-T, and the Artemis II optical communications programs—have validated the operational viability of optical networking across multiple mission sets.⁴⁶ Industry is advancing in parallel. Companies such as General Atomics Electromagnetic Systems, CACI, Mynaric, and Blue Marble Communications are developing optical terminals capable of data transmission rates approaching or exceeding 100 gigabits per second and scaling production for proliferated constellations.⁴⁷ Taken collectively, this reveals that optical communications have matured from promising technology demonstrations into operational transport architectures capable of supporting future military and commercial space networks. While government and industry demonstrations indicate growing technical maturity, transitioning these capabilities into operational architectures will require overcoming acquisition, integration, and programmatic challenges. Commercial providers are accelerating the transition to hybrid architectures.

Commercial providers are accelerating the transition to next-generation space communications architectures at a pace that traditional government acquisition programs often cannot match. Rapid hardware iteration, software updates, and deployment at constellation scale are allowing industry to demonstrate operational concepts years before comparable government systems reach the field. The RAND Corporation has concluded that commercial integration is becoming foundational to future military space architectures because commercial providers can deliver capabilities at speeds, scales, and costs that government-only approaches struggle to achieve.⁴⁸ Starlink provides the clearest example.

With more than 10,000 satellites launched and roughly 9,000 currently active in LEO, SpaceX's Starlink constellation represents the largest satellite network ever deployed and accounts for more than half of all active satellites in orbit as of mid-2026.⁴⁹ This unprecedented scale reflects the accelerating role commercial providers are playing in the development of next-generation communications architectures, particularly in areas such as proliferated constellations, optical inter-satellite links, cloud-enabled data transport, and globally distributed mesh networking.

Advanced Networking Concepts & Why They Matter

Building a hybrid RF-optical architecture is only the first step. Future military communications networks must also intelligently manage how information moves across multiple communications pathways. As RF and optical links become available or unavailable for use due to congestion, degradation or interference, the network must determine when to transmit data, which pathway to use, and when to temporarily store information until a better route becomes available. Advanced networking concepts such as Delay/Disruption Tolerant Networking (DTN) and multi-user relay operations enable this dynamic management.

Delay/Disruption Tolerant Networking (DTN) is designed to move data reliably across communications environments where connections may be intermittent, delayed, or temporarily unavailable. Rather than requiring a continuous end-to-end connection, DTN stores data until a viable transmission pathway becomes available, helping maintain information flow across distributed space networks.

Multi-user relay operations allow a communications relay system to receive, manage, and transmit data from multiple users simultaneously. This capability improves network efficiency and enables a single relay architecture to support numerous satellites, sensors, and operational users across a shared communications infrastructure. These networking concepts improve the resilience, flexibility, and scalability of future space communications architectures, helping to ensure that mission-critical information continues to move even when portions of the network are degraded, congested, or temporarily disconnected.

The operational implications of these commercial architectures are already becoming visible. Starlink's optical mesh network enables data to move globally across thousands of interconnected satellites without immediate dependence on terrestrial relay infrastructure. In 2024, SpaceX expanded these capabilities beyond its own constellation by offering optical terminals to third-party satellite operators. California-based Muon Space subsequently announced plans to integrate these terminals into its Halo architecture, enabling direct connectivity to Starlink's optical mesh network at data transmission rates of up to 25 gigabits per second over distances approaching 4,000 kilometers.⁵⁰ According to Muon, this approach could increase network availability from roughly 10–30 percent to 70–80 percent while reducing data-delivery timelines from approximately 20 minutes to near real-time. These developments reveal how commercial optical networks are evolving into globally distributed data-transport infrastructures capable of supporting latency-sensitive operations at scale.

Even dramatically expanding transport capacity is only part of the solution. Future military networks must not only move more data but also manage that data more intelligently. As data generation continues to accelerate, architectures that filter, prioritize, compress, and route information before transmission will become more important to sustaining operational effectiveness across constrained communications networks.

Line of Effort 2: Use Intelligent Processing to Move Less Data, Faster

Reducing the burden on communications networks will require future architectures to become more efficient at processing, managing, storing, and transmitting information. A growing set of technologies—including onboard processing, AI-enabled analytics, data compression, on-orbit data management, and distributed commercial networks—can reduce transmission requirements while preserving the operational value of time-sensitive data. Table 8 summarizes the principal approaches currently being explored to reduce communications burdens and improve information flow across data-intensive military architectures.

Technique	Function	Operational Benefit	Communications Impact	Example
Onboard processing	Filters data before transmission	Reduces transport of unnecessary data	Preserves bandwidth	NASA LCRD/ILLUMA-T relay architecture
AI-enabled edge computing	Processes data near collection	Accelerates decision timelines	Reduces latency	Emerging AI-enabled ISR & Missile Warning architectures
Compression and smart encoding	Reduces redundancy in transmissions	Improves throughput efficiency	Maximizes finite bandwidth	NASA deep-space communications architectures
On-orbit storage and routing	Stores/routes data within the network	Reduces reliance on constant downlink	Reduces transport burden	Orbital data-center concepts supporting Golden Dome architectures
Distributed commercial architectures	Routes/processes data across proliferated networks	Improves resiliency and persistence	Demonstrates operational feasibility	SpaceX Starlink optical mesh network

Table 8: Data-burden reduction techniques.

Onboard processing reduces transmission burdens through data filtering and prioritization. One of the most effective ways to relieve pressure on communications networks is to reduce the amount of data requiring transmission in the first place. Onboard processing accomplishes this by analyzing information at or near the point of collection rather than transmitting all raw sensor data to centralized processing centers. These systems perform automated data triage, determining which information must be transmitted immediately, which can be compressed or delayed, and which may not require transmission at all. Rather than saturate networks with raw sensor feeds, future architectures must transmit prioritized alerts, refined data products, and mission-relevant information tailored to operational requirements.

The benefits are already evident across military and civil remote-sensing systems. Earth-observation satellites equipped with hyperspectral imaging, synthetic aperture radar, and persistent sensing payloads generate enormous quantities of raw data, much of which may never require transmission or human review. By filtering, compressing, and prioritizing information before transmission, onboard processing reduces unnecessary downlink requirements while preserving the information most critical to mission success.⁵¹ Similar approaches are being applied to disaster response and environmental monitoring. These enable faster identification of fires, flooding, infrastructure damage, and other time-sensitive events without continuously transmitting large volumes of raw imagery.⁵² Together, these developments reflect a broader shift from transmitting everything that is collected to transmitting only the information that matters most.

AI and edge computing accelerate decision advantage. Reducing transmission demands is only part of the challenge. As operational timelines continue to compress, military architectures must convert collected data into actionable information before opportunities disappear. AI-enabled edge computing addresses this challenge by processing, analyzing, and exploiting data within the network itself rather than relying exclusively on centralized ground-based analysis. By identifying patterns, detecting anomalies, prioritizing mission-relevant information, and generating actionable outputs near the point of collection, these systems reduce latency, lessen analyst workload, and accelerate decision-making.

Emerging wildfire-monitoring architectures establish the operational potential of onboard AI-enabled processing. In one recent demonstration, an AI-enabled small satellite reduced wildfire detection timelines by approximately a factor of 500 while reducing the volume of downlinked data to roughly 16 percent of its original size.⁵³ Rather than transmitting massive volumes of raw imagery for later analysis, the satellite identified mission-relevant indicators onboard and transmitted only prioritized information.

The greatest near-term value of AI-enabled edge computing lies not in replacing human judgment, but in reducing the volume of data that must be transmitted and ensuring that analysts and commanders receive the most relevant information more quickly. Applications such as data filtering, anomaly detection, sensor cueing, and information prioritization are well suited to onboard AI processing. Conversely, more complex operational decisions involving adversary deception, ambiguous conditions, or the use of force will continue to rely on human oversight.

As retired Lt Gen Nina Armagno and former U.S. Space Force Chief Data Officer retired Maj Gen Kim Crider argue, future space operations will depend on machine-speed decision-making enabled by AI-driven architectures capable of managing and exploiting large volumes of data within the operational network itself.⁵⁴ RAND analysis reaches a similar conclusion, identifying edge processing and intelligent data management as essential to sustaining distributed operations under constrained bandwidth conditions.⁵⁵

Data compression and smart encoding improve the efficiency of constrained communications pathways. Improving the efficiency of existing communications pathways offers an immediate means of relieving network congestion. Data compression and advanced encoding techniques reduce redundancy and maximize the amount of usable information transmitted within each communications link, enabling networks to carry more operationally relevant data without requiring additional bandwidth. Rather than expanding transport capacity, these approaches improve the efficiency of existing communications architectures by enabling more information to move over finite pathways.

NASA's deep-space communications architecture already relies on advanced encoding and compression techniques to maximize the amount of scientific and operational data transmitted across highly constrained links spanning enormous distances.⁵⁶ Similar challenges are emerging within proliferated Earth-observation and military sensing architectures, where hyperspectral imaging, SAR, and persistent ISR systems can generate data volumes that exceed available downlink capacity. As an example, one advanced SAR satellite system under development is projected to produce approximately 200,000 gigabytes of data per day, while the supporting downlink rate is only 86,400 gigabits per day (a 1-Gbps link).⁵⁷ This system will essentially generate more than 18 times as much data as can be transmitted currently through available communications links. Advanced compression and encoding techniques therefore are needed to complement broader efforts to expand transport capacity and reduce transmission burdens.

On-orbit data storage and routing reduce reliance on continuous raw data transmission. Commercial firms and defense planners are exploring orbital data centers and distributed processing architectures designed to process, store, and route information directly within space-based networks. Instead of continuously transmitting massive volumes of raw data to Earth for analysis, these architectures perform portions of data processing, storage, and routing within the network itself, reducing bandwidth requirements, lowering latency, and accelerating the delivery of operationally relevant information across distributed systems.⁵⁸ This approach is particularly attractive

for future multi-orbit architectures expected to support highly distributed and latency-sensitive operations such as missile warning, missile defense, and globally integrated command and control.

The operational implications are especially significant as emerging threats—including maneuverable and hypersonic weapons—continue compressing decision timelines. By reducing unnecessary transport requirements and enabling analysis closer to the point of collection, on-orbit storage and routing architectures offer a pathway toward faster sensor-to-decision timelines.⁵⁹ However, many emerging orbital computing-based architectures operate with differing standards, fragmented governance approaches, and limited interoperability between networks.⁶⁰ Without common frameworks for certification, interoperability, and data management, the long-term scalability of distributed on-orbit processing architectures will remain constrained despite growing interest in the concept. U.S. leadership in developing these standards will be strategically important not only for ensuring interoperability across military, allied, and commercial architectures, but also for shaping the trusted communications ecosystem on which future coalition operations will depend.

Commercial architectures demonstrate scalable data management. Commercial space architectures have already demonstrated that distributed data management in orbit is operationally achievable at an unprecedented scale. SpaceX's Starlink constellation, for example, routes information across thousands of interconnected satellites through its optical mesh network, allowing data to traverse the constellation before reaching the most effective downlink location.⁶¹ Commercial providers are also extending these capabilities by integrating cloud-computing and edge-processing concepts into space-based networks. Microsoft's Azure Orbital Cloud Access, for instance, seeks to connect space assets directly with cloud infrastructure, enabling more efficient management and exploitation of space-derived data.⁶² Although developed for commercial applications, these systems already demonstrate many of the architectural principles required for future military communications networks.

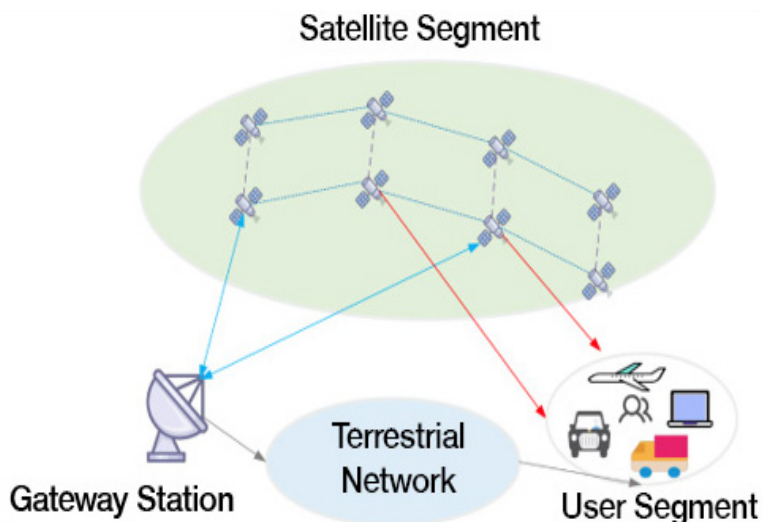


Figure 14: Distributed data routing through a space-based mesh network. By routing information through alternate pathways when needed, mesh networks improve communications resilience and demonstrate key architectural principles underlying future distributed processing and data-management systems in space.

Image credit: CC BY 4.0: Cao, Xiaoli, Yitao Li, Xingzhong Xiong, and Jun Wang, "Dynamic Routings in Satellite Networks: An Overview," *Sensors* 22, no. 12:4552.

For military forces operating in degraded, disconnected, or bandwidth-constrained environments, these developments illustrate how distributed networks can maintain resilient information flow, even when individual nodes or terrestrial infrastructure becomes unavailable.⁶³ As distributed sensing systems and latency-sensitive missions continue to expand, commercial architectures demonstrate that intelligent routing and distributed data management can reduce transmission burdens while improving operational resilience.

Line of Effort 3: Optimize & Extend RF Performance

Because the joint force will remain heavily dependent on RF communications for the foreseeable future, improving the resilience and efficiency of existing RF architectures remains operationally essential, even as next-generation hybrid RF-optical systems mature. Military operations continue to rely on RF communications for command and control, navigation, sensing, targeting, missile warning, and distributed coordination across globally integrated forces. The challenge, therefore, is not replacing RF systems outright, but improving their survivability, adaptability, security, and efficiency while integrating them into higher-capacity hybrid architectures. Efforts such as anti-jam waveforms, spectrum agility, encryption, and proliferated downlink architectures strengthen RF performance and ensure an RF capability remains an effective component of future communications networks (see Table 9). Although these approaches cannot eliminate the inherent limitations of a finite spectrum, RF observability, or growing transport demands, they significantly extend the operational effectiveness of RF systems while optical capabilities continue to mature.

Anti-jam and resilient waveforms improve the survivability of communications in contested electromagnetic environments. Improving the survivability of RF communications is essential to sustaining operational effectiveness in contested environments. The Department of Defense/War's Electromagnetic Spectrum Superiority Strategy emphasizes that future systems must be capable of operating even as an adversary attempts to disrupt, degrade, or deny electromagnetic access through jamming, interference, spoofing, and other forms of electronic warfare.⁶⁴

Meeting this requirement demands RF systems that can adapt dynamically to contested conditions rather than relying on fixed transmission methods or static operating frequencies. Anti-jam and resilient waveform approaches—including spread-spectrum techniques, frequency hopping, low-probability-of-intercept/low-probability-of-detection (LPI/LPD), adaptive modulation, advanced coding, and interleaving—are designed to complicate adversary targeting and improve communications survivability within contested electromagnetic environments. Protected Tactical Waveform (PTW) systems, which employ many of these techniques, are designed to maintain connectivity even during active jamming attempts. By dynamically adjusting transmission characteristics, they force adversaries to expend significantly greater effort and power to disrupt communications.⁶⁵ These techniques cannot eliminate the observable nature of RF transmissions or fully prevent interception and interference, but they do make military communications significantly more difficult to disrupt. These adaptive measures therefore improve resilience during contested operations.

Spectrum agility improves efficiency within congested and contested frequency bands. As spectrum congestion intensifies, improving RF performance will depend on using the available spectrum more efficiently rather than simply expanding access to additional bandwidth. Modern RF systems rely on spectrum agility to adapt

Technique	Problem Addressed	Benefit	Limitation	In Use Examples
Anti-jam/spread spectrum waveforms	Jamming/survivability	Improves communications survivability in contested EM environments	Cannot eliminate RF observability or spectrum constraints	Protected Tactical Waveform/ Protected Tactical SATCOM
Adaptive coding, modulation, and dynamic spectrum allocation	Spectrum congestion, interference, and changing operating conditions	Improves spectrum efficiency, throughput, and resilience by adapting transmissions to environmental conditions	Increases system complexity; many cognitive radio capabilities remain operationally immature	DVB-S2/DVB-S2X satellite links NASA Cognitive radio/ AI-enabled space communications research; DARPA CommEX cognitive radio concepts NASA SCA _N spectrum-management (Digital Video Broadcasting; example: DirecTV)
Encryption and secure communication	Data interception and exploitation	Protects the confidentiality, integrity, and authenticity of operational data while preserving communications under contested conditions	Does not increase bandwidth or overcome jamming; requires robust key management	Protected Tactical Waveform/ Protected Tactical SATCOM Commercial National Security Algorithm (CNSA) Suite
Proliferated downlink architectures	Data bottlenecks	Expands access points and reduces bottlenecks	Requires additional infrastructure and network coordination	AWS' ground stations (Amazon), KSAT global ground network (Norway), NASA smallsat ground-services

Table 9: RF techniques: valuable but limited.

Example data adapted from NASA SCA_N, MITRE, ITU publications, DARPA communications research, ETSI standards documentation, and SSC analyses: see John Stine and David Portigal, *Spectrum 101*, MITRE Technical Report (The MITRE Corporation, March 2004); "CommEx: Communications Under Extreme Spectrum Conditions," Strategic Technology Office, DARPA, accessed June 10, 2026; Jayaweera et al., "Cognitive Anti-jamming Satellite-to-Ground Communications on NASA's SCA_N Testbed"; "DVB-S2 vs DVB-S2X," *everything RF*, January 8, 2023; National Security Agency Central Security Service, "Commercial National Security Algorithm (CNSA) Suite," accessed July 22, 2026; Caleb Henry, "AWS completes six ground stations, changes rollout strategy," *Space News*, August 4, 2020; and "Global Ground Station Network," Kongsberg Satellite services, accessed June 10, 2026.

automatically to changing operational conditions. Techniques such as frequency hopping, adaptive modulation, dynamic spectrum management, and emerging cognitive radio capabilities enable communications systems to avoid interference, share bandwidth more efficiently, and maintain connectivity even in congested and contested environments (see Table 9). Together, these approaches improve the efficiency and flexibility of RF architectures and reduce their susceptibility to interference and localized congestion. They do not, however, increase the amount of spectrum available, leaving the fundamental limitations of finite RF bandwidth unresolved.

Proliferated downlink architectures reduce bottlenecks and improve network resilience. Proliferated downlink stations and architectures are emerging as an important means of reducing communications bottlenecks and improving network resilience. As the number of operational satellites has increased dramatically over the past three decades, the legacy ground-based infrastructure and architectures have remained largely unchanged. Traditional communications systems often rely on relatively few centralized ground stations and downlink antennas capable of receiving and processing satellite data. As proliferated constellations and advanced sensing systems generate

increasing volumes of operational data, limited ground access points are becoming bottlenecks that constrain how quickly information can be delivered to operational users. Expanding data transport across geographically dispersed downlink stations, relay pathways, and interconnected communications assets reduces congestion, improves scalability, and provides alternate pathways when individual nodes become unavailable.⁶⁶

Commercial ground networks, hybrid cloud-enabled transport systems, and planned proliferated military architectures demonstrate the advantages of this more distributed approach. At its most basic level, this means building more downlink antennas, ground stations, and the terrestrial fiber infrastructure needed to move data rapidly once it reaches Earth. By expanding the number of available ground access points and reducing dependence on any single transmission pathway, proliferated downlink architectures improve resilience, distribute network load more efficiently, and accelerate the movement of operational data across globally integrated military operations.

Together, these RF optimization approaches can significantly improve the survivability, efficiency, security, and resilience of military communications while extending the operational utility of RF-based systems. They do not, however, overcome the fundamental constraints of finite spectrum, RF observability, or rapidly growing transport demand. As military operations become more data-intensive, future communications architectures must combine these enduring RF capabilities with higher-capacity optical transport networks to deliver the scale, resilience, and flexibility required for modern warfare.

Encryption and data protection improve the security and integrity of operational data flows. Although proliferated and distributed architectures improve resilience by reducing single points of failure, they also increase the number of network nodes, communications pathways, and interfaces through which operational data move, creating additional avenues for cyber intrusion and data exploitation. Recognizing this expanding attack surface, the Department of Defense/War identifies RF-enabled cyber threats and electromagnetic exploitation as growing operational risks.⁶⁷ As previously mentioned, Russia's 2022 cyberattack against the ViaSat satellite network disrupted communications across portions of Europe, degrading operations ranging from Ukrainian military drones to German wind turbines.⁶⁸ Similarly, in April 2024, Russian hackers reportedly hijacked satellite television broadcasts across Europe, replacing normal programming with propaganda and demonstrating the vulnerability of commercial satellite communications to intrusion and exploitation.⁶⁹

Modern communications systems must therefore protect not only the communications pathway but also the integrity, confidentiality, and availability of the data moving across it. Encryption, secure transmission protocols, hardened network architectures, and protected data-handling procedures help ensure that operational information remains trustworthy, protected, and usable in contested environments. These measures become more important as proliferated architectures, spectrum sharing, and commercial integration create additional opportunities for cyber intrusion and electromagnetic exploitation. Although encryption and data protection do not increase throughput or reduce transport bottlenecks, they remain essential to preserving confidence in the integrity and reliability of information moving across more complex military communications networks.

Challenges & Considerations for Implementation

Modernizing military communications architectures will require more than technological innovation. Hybrid RF-optical networks introduce increased operational complexity, demand sustained institutional and financial commitment, and require adaptation across military, commercial, and allied ecosystems. At the same time, delaying modernization increases operational vulnerability and diminishes the United States' ability to shape the future communications environment.

Delayed Adoption Carries Strategic Risk

The strategic risks associated with delaying communications modernization increasingly outweigh the operational, financial, and institutional challenges of transition with each budget cycle. Operational data demands continue to increase as both commercial providers and U.S. competitors invest heavily in proliferated satellite networks, distributed communications ecosystems, and hybrid transport architectures. As the communications environment evolves, timely architectural modernization becomes more important to maintaining long-term operational and strategic advantage. Early adoption of emerging communications architectures will shape the interoperability standards, integration frameworks, and operational assumptions that define future military communications ecosystems. Again, the competition over 5G standards perfectly illustrates how leadership in foundational technologies translates into broader strategic influence, with nations that shape technical standards likewise influencing the ecosystems built upon them.⁷⁰ If the United States does not want China or other nations to dictate the standards and compliance terms of hybrid architectures, then it must be an early leader in fielding these networks.

Modernization Will Require Sustained Investment & Adaptive Acquisition Approaches

Communications modernization will require immediate investment and sustained funding across multiple budget cycles. Because legacy RF systems will remain operationally necessary while hybrid communications architectures mature, the services must simultaneously sustain existing capabilities while investing in future architectures. Stable resourcing, continued commercial participation, and long-term institutional commitment to both legacy RF capabilities and hybrid/optical technologies will be essential to avoid modernization gaps and ensure communications capabilities evolve alongside growing operational demands. Communications modernization is therefore not a one-time procurement effort, but a sustained strategic investment in future military effectiveness.

Legacy RF-based communications systems remain deeply embedded within military operations and cannot be replaced abruptly without introducing operational risk. Existing command-and-control pathways, satellite communications networks, and supporting infrastructure must continue providing mission-essential connectivity while hybrid communications architectures are integrated and operationalized. Modernization will require a transition period during which legacy and emerging architectures operate simultaneously. Although this will increase operational, financial, and architectural complexity, it is a necessary course of action.

Some of this complexity is due to the fact that communications technologies continue evolving faster than traditional acquisition and budgeting processes were designed to accommodate. Successfully modernizing communications architectures will require acquisition approaches that can adapt to rapidly evolving commercial capabilities, operational requirements, and technological advances while maintaining the reliability and mission assurance required for military operations. Achieving this will require greater use of iterative acquisition, spiral development, rapid prototyping, and operational experimentation. In this way, communications architectures can evolve as technologies mature rather than waiting for fully developed end-state solutions.

Integrating Hybrid Architectures Increases Operational & Network Complexity

Hybrid RF-optical architectures improve resilience, scalability, and survivability, but they also increase operational and network-management complexity. Successfully integrating military, allied, and commercial communications networks will require interoperable standards, common integration frameworks, and sophisticated routing and orchestration requirements across multiple transport pathways. Because future communications architectures will rely upon a combination of military, allied, and commercial systems, interoperability standards established today will significantly influence integration costs, operational flexibility, and long-term architectural compatibility.

The growing role of commercial providers and proliferated communications architectures further increases the importance of standards development, network coordination, and enterprise-level integration.⁷¹ Without sufficient coordination, hybrid architectures risk becoming collections of technically connected systems that remain operationally difficult to integrate, manage, and scale across globally distributed operations.

Recommendations & Conclusion

Recommendation 1: Accelerate & Sustain Communications Modernization Through Stable Resourcing & Adaptive Acquisition

The Department of Defense/War and the U.S. Space Force should treat communications modernization as a long-term operational imperative and resource it accordingly. It must be supported by stable long-term investment, adaptive acquisition approaches, and deliberate integration of legacy and emerging capabilities. The central requirement is not simply to fund new technologies, but to create the institutional, budgetary, and acquisition conditions necessary to field resilient hybrid RF-optical architectures at operational scale. Because RF systems will remain essential for the foreseeable future, modernization should focus on a deliberate transition that preserves current mission effectiveness while building the capacity, resilience, and flexibility required for future conflict.

Efforts to build this foundation should prioritize:

- Sustaining communications modernization investments across current and future budgets, force-design, and capability-development efforts to ensure hybrid architectures mature alongside operational demand.
- Expanding acquisition approaches that allow communications architectures to evolve alongside rapidly advancing commercial technologies and changing operational requirements.
- Strengthening the commercial and industrial base needed to support proliferated communications, optical transport, adaptive RF architectures, and distributed networking ecosystems.
- Embedding communications modernization within long-term force design, capability development, and resource planning to ensure enduring investment across future budget cycles.

Communications superiority will depend on choices made well before future conflict begins. Stable resourcing, adaptive acquisition, and deliberate investment in hybrid architectures are therefore essential to preserving operational flexibility and strategic advantage over time.

Recommendation 2: Operationalize Hybrid RF-Optical Architectures Across the Force

The Department of Defense/War and the U.S. Space Force should accelerate the operational integration of hybrid RF-optical communications architectures into real-world military practice. The challenge is no longer demonstrating the technology; it is integrating it into military operations. As proliferated sensing, persistent tracking, distributed operations, and data-intensive kill webs continue to expand, communications demands are outpacing the practical limits of RF-centric architectures alone. Hybrid architectures must therefore be incorporated into operational concepts, training, exercises, network management practices, and day-to-day force employment so that they become operational capabilities rather than merely promising technical concepts.

Efforts to operationalize hybrid architectures should prioritize:

- Expanding operational experimentation and demonstrations that integrate hybrid RF-optical architectures into realistic joint and combined scenarios.
- Developing concepts of operation, network-management approaches, and employment models for contested and degraded communications environments.
- Integrating intelligent processing, data prioritization, compression, advanced encoding, and adaptive routing to reduce transport burdens across data-intensive operations.
- Continuing to improve RF performance through resilient waveforms, spectrum agility, and proliferated networking so that existing systems remain effective within future hybrid architectures.
- Leveraging relevant commercial capabilities and lessons from proliferated and distributed communications architectures already in use.
- Continuing to address the remaining technical challenges associated with optical communications, including weather effects, precision pointing and tracking, routing flexibility, and resilient multi-path transport.

Technology alone will not deliver future communications superiority. Operational advantage will depend on whether hybrid architectures are integrated with how the force trains, plans, and fights before future conflicts expose the consequences of delay.

Recommendation 3: Lead Interoperability & Standards Development for the Future Communications Ecosystem

The Department of Defense/War and the U.S. Space Force should take a deliberate leadership role in shaping interoperability standards, integration frameworks, and partnership models that will define the future of military communications ecosystems. Future advantage will depend not only on transport capacity, but also on the ability to move, route, process, and exploit data seamlessly across military, allied, commercial, and multi-domain networks operating within contested environments. Hybrid RF-optical architectures will deliver their full value only if they are embedded within interoperable, scalable, and resilient communications ecosystems. Because these standards and integration frameworks become difficult to change once widely adopted, the United States must act early to help shape the communications ecosystem in ways that accelerate innovation and support long-term strategic advantage.

Efforts to lead this ecosystem should prioritize:

- Expanding interoperability standards and integration frameworks that support hybrid RF-optical architectures across military, allied, and commercial networks.
- Strengthening collaboration with commercial providers that are advancing proliferated networking, distributed routing, and hybrid communications capabilities relevant to future military operations.
- Improving coalition and partner integration to better support future communications architectures for combined and allied operations.
- Encouraging vendor-agnostic and pathway-diverse architectures that reduce dependence on singular transport links, providers, or technical solutions.
- Integrating interoperability, distributed routing, and resilient network management into future communications architecture development and operational planning.

Future military effectiveness will depend on connecting the most capable ecosystem, not simply fielding the most capable individual system. By leading the development of interoperability standards and integration frameworks, the Department of Defense/War can strengthen coalition effectiveness, accelerate innovation, and shape the communications environment in ways that favor U.S. and allied operations.

Conclusion

The character of modern warfare is changing faster than the communications architectures that support it. Distributed operations, proliferated sensing, persistent tracking architectures such as AMTI/GMTI, joint all-domain operations, and data-intensive kill webs are generating demands for speed, scale, persistence, and survivability that exceed the limitations of many legacy military communications systems. In this environment, the ability to move, protect, process, and exploit information at scale is no longer a supporting function; it is a prerequisite for operational effectiveness.

RF-based architectures will remain essential to military operations and will continue to play a central role in future communications ecosystems, but incremental improvements to RF capabilities in spectrum efficiency, anti-jam performance, waveform design, and network management will not be sufficient on their own to meet the demand. The scale and persistence of modern data generation are outpacing the capacity of legacy RF-centric architectures to support them efficiently, even as adversaries' counterspace, cyber, and electronic warfare capabilities increase the vulnerability and observability of those systems. Closing this gap will require hybrid communications ecosystems that combine RF optimization, optical transport, intelligent processing, distributed routing, and interoperable network management across military, allied, and commercial architectures. Optical communications are not a replacement for RF systems, but a critical enabling capability within a more resilient and scalable hybrid architecture.

The strategic question, then, is not whether military communications architectures must evolve, but whether the United States will move fast enough to preserve decision advantage before the gap widens further. Competitors are already investing in proliferated communications networks, hybrid transport architectures, and data-centric operational concepts designed for contested environments. If the United States delays, it risks ceding not only operational advantage, but also influence over the standards, architectures, and partnerships that will shape future military communications.

Communications superiority is becoming inseparable from operational superiority. The force that can transport, prioritize, protect, and exploit mission-relevant information at speed and scale will be better positioned to coordinate distributed operations, absorb disruption, and maintain decision advantage in future conflict. The decisions made now—on architecture, interoperability, acquisition, and investment—will determine whether future military forces merely cope with the communications demands of tomorrow's battlespace or decisively wield them for operational dominance.



Figure 15: Optical communications in multiple domains.

Credit: GA-EMS

Endnotes

- 1 National Intelligence Council, [“Deeper Looks: The Future of the Battlefield.”](#) Global Trends 2040: A More Contested World, March 2021.
- 2 [“Electromagnetic Spectrum Superiority Strategy.”](#) Department of Defense (DOD), October 2020.
- 3 Victoria Samson, [“Global Counterspace Capabilities 2026.”](#) Secure World Foundation, April 2026.
- 4 David Klepper, [“Space is the new battlefield with hijacked satellites and orbiting weapons.”](#) *PBS News*, August 18, 2025.
- 5 Courtney Albion, [“Space Force Resets Modernization Plan for Its Aging Satellite Control Network.”](#) *Air & Space Force Magazine*, April 7, 2026.
- 6 [“Chapter VI: Air Force Satellite Control Network.”](#) May 2, 2016.; and NASA, [“USA Space Debris Environment, Operations, and Modeling Updates.”](#) February 22, 2013.
- 7 Heather R. Penney, *Scale, Scope, Speed & Survivability: Winning the Kill Chain Competition* (Arlinton, VA: the Mitchell Institute for Aerospace Studies, May 2023).
- 8 Vivienne Machi, [“US Military Places a Bet on LEO for Space Security.”](#) *Via Satellite*, June 2021.
- 9 Victoria Samson, [“Global Counterspace Capabilities 2026.”](#) Secure World Foundation, April 2026.
- 10 Jake Epstein, [“Ukraine’s digital war tool cut the time between finding and striking Russian targets from days to minutes.”](#) *Business Insider*, November 24, 2025.
- 11 Samson, [“Global Counterspace Capabilities 2026.”](#)
- 12 [“Summary of the Joint All-Domain Command and Control \(JADC2\) Strategy.”](#) DOD, March 2022.
- 13 Penney, *Scale, Scope, Speed & Survivability*.
- 14 John Hoehn, *Joint All-Domain Command and Control: Background and Issues* (Washington, DC: Congressional Research Service [CRS], August 12, 2021).
- 15 Sandra Erwin, [“Saltzman: Space ‘baked into’ modern combat operations.”](#) *Space News*, April 1, 2026.
- 16 Mark Pomerleau, [“Proliferated LEO, hybrid cloud capabilities enable U.S. forces to operate more disconnected.”](#) *Defense Scoop*, October 22, 2024.
- 17 U.S. Space Force, [“Future Operating Environment 2040.”](#) April 25, 2026.
- 18 U.S. Coast Guard, [“Electromagnetic Spectrum Management Operations in the Electromagnetic Environment.”](#) U.S. Department of Homeland Security, September 9, 2022.
- 19 Nicholas Johnson, [“Back to the Future of Comms.”](#) RAND Commentary, July 30, 2024.
- 20 Samson, [“Global Counterspace Capabilities 2026.”](#)
- 21 The consequences of spectrum disruption are measurable outside purely military contexts. As mentioned previously, a UK study estimated that a 24-hour outage of Global Navigation Satellite Systems (GNSS) would cause approximately 1.4 billion pounds in economic losses. In comparison, a seven-day outage could generate losses exceeding 7.6 billion pounds. Identified likely downstream operational consequences included degraded emergency location services, approximately 19,000 unanswered emergency calls during a prolonged outage , and other severe logistics disruptions. RF vulnerability is an already observable operational challenge with significant military, economic, and societal consequences. Rasmus Flytkjaer et al., *The economic impact on the UK of a disruption to GNSS* (London: London Economics, August 2023).
- 22 Andre Doumitt and Laura Speckman, *Lasercom Key to Building Internet in Space: Government and Private Sector Poised to Scale* (El Segundo, CA: Aerospace Corporation, 2023).
- 23 [“Summary of the Joint All-Domain Command and Control \(JADC2\) Strategy.”](#)
- 24 Penney, *Scale, Scope, Speed & Survivability*.
- 25 [“Proliferated Warfighter Space Architecture \(PWSA\): Tracking Layer.”](#) Space Development Agency, August 2024.
- 26 [“Proliferated Warfighter Space Architecture \(PWSA\): Tracking Layer.”](#)
- 27 Mamata Akella, [“The 9 top satellite imagery companies.”](#) *Felt* blog, December 1, 2025.
- 28 Waleed Abdalati, William B. Gail, et al., *Thriving on Our Changing Planet: A Decadal Strategy for Earth Observation from Space*, Consensus Study Report (Washington, DC: The National Academies Press, 2018), p. 19.
- 29 LEO Policy Working Group, [“A Brief Introduction to Low Earth Orbit \(LEO\) Satellites.”](#) New America, January 2025.
- 30 Doumitt and Speckman, *Lasercom Key to Building Internet in Space*.
- 31 Doumitt and Speckman, *Lasercom Key to Building Internet in Space*.
- 32 Emily Kilcrease and Adam Tong, *Disorderly Conduct: How U.S.-China Competition Upended the International Economic Order & What the U.S. Can Do to Fix It* (Washington, DC: Center for a New American Security, June 2024).
- 33 Samson, [“Global Counterspace Capabilities 2026”](#); and U.S. Space Force, [“Space Threat Fact Sheet.”](#) current as of July 2026.
- 34 Andrew Jones, [“Large Series C signals scale-up of China’s laser satellite communications sector.”](#) *Space News*, March 11, 2026.
- 35 American National Standards Institute, [“United States Standards Strategy 2025.”](#) January 2026.
- 36 James Andrew Lewis and Clete Johnson, *Accelerating 5G in the United States: CSIS Working Group on Trust and Security in 5G Networks* (Washington, DC: Center for Strategic and International Studies, March 1, 2021).
- 37 Nicol Lee Turner, [“Navigating the U.S.-China 5G Competition.”](#) in, *Global China: Assessing China’s Growing Role in the World* (Washington, DC: The Brookings Institute, April 2020).
- 38 Owais Ali, [“How is Laser Communication Used in Space?”](#) *AZO Optics*, September 13, 2023.
- 39 Doumitt and Speckman, *Lasercom Key to Building Internet in Space*.

- 40 Kimberly Burke, [“A Quilty Space Insight: How Amazon Kuiper is Gearing up to Break the Bandwidth Bottleneck.”](#) *Quilty Space*, December 14, 2023, updated April 22, 2025.
- 41 Courtney Albon, [“Space Development Agency demos key space-to-air communications link.”](#) *Defense News*, September 2, 2025.
- 42 Theresa Hitchens, [“Hypersonics: SDA, Space Force Focus on Laser Links For Kill Chain.”](#) *Breaking Defense*, December 8, 2020.
- 43 Jon Ludwigson, [“Laser Communications: Space Development Agency Should Create Links Between Development Phases”](#) (Washington, DC: GAO, February 2025).
- 44 Kendall Murphy and Katherine Schauer, [“NASA’s First Two-way End-to-End Laser Communications Relay System.”](#) NASA, October 25, 2023.
- 45 Shaun Waterman, [“Space Lasers Come of Age: Optical Communications for Satellites Are Ready for Prime Time.”](#) *Via Satellite*, February 22, 2022.
- 46 Ariana Gaines, [“Lincoln Laboratory laser communications terminal launches on historic Artemis II moon mission.”](#) *MIT News*, April 2, 2026; and Murphy and Schauer, [“NASA’s First Two-way End-to-End Laser Communications Relay System.”](#)
- 47 Sandra Erwin, [“U.S. Space Force narrows field in \\$100 million space laser terminal program.”](#) *Space News*, May 8, 2025.
- 48 Johnson, [“Back to the Future of Comms.”](#)
- 49 “How Many Starlink Satellites Are in Orbit?” *Orbital Radar*, accessed May 22, 2026.
- 50 Jason Rainbow, [“Starlink mini lasers to link Muon Space satellites for near real-time connectivity.”](#) *Space News*, October 21, 2025.
- 51 Aravind, [“Edge Computing for Earth Observation – 2026 Edition.”](#) *Terrawatch Space*, February 27, 2026.
- 52 [“AI-Enabled Onboard Edge Computing for satellite Intelligence in Disaster Management.”](#) Office for Outer Space Affairs, UN-SPIDER Knowledge Portal, United Nations, November 5, 2025.
- 53 University of South Australia, [“Fighting fires from space in record time: how AI could prevent devastating wildfires.”](#) *Newswise*, June 5, 2024.
- 54 Nina Armagno, and Kim Crider, [“Agentic AI: the future of space warfare.”](#) *Space News*, March 31, 2026.
- 55 Kim Yool et al., [“Operational and Policy Implications of Integrating Commercial Space Services into U.S. Department of Defense Operations”](#) (Santa Monica, CA: RAND Corporation, February 11, 2025).
- 56 Katherine Schauer, [“Space Communications: 7 Things You Need to Know.”](#) NASA, October 6, 2020.
- 57 Laura Garcia Parra et al., [“Advancements in On-Board Processing of Synthetic Aperture Radar \(SAR\) Data: Enhancing Efficiency and Real-time Capabilities.”](#) *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing* 17, March 2024.
- 58 Courtney Albon, [“Data Centers Could Enable Golden Dome: Experts.”](#) *Air & Space Forces Magazine*, March 27, 2026.
- 59 Albon, [“Data Centers Could Enable Golden Dome: Experts.”](#)
- 60 John David Callison and Joseph Minfra, [“The governance gap: Why orbital data centers need certification before they scale.”](#) *Space News*, April 24, 2026.
- 61 Pomerleau, [“Proliferated LEO, hybrid cloud capabilities enable U.S. forces to operate more disconnected.”](#)
- 62 Jason Zander, [“New Azure Space products enable digital resiliency and empower the industry.”](#) Microsoft, September 14, 2022.
- 63 Pomerleau, [“Proliferated LEO, hybrid cloud capabilities enable U.S. forces to operate more disconnected.”](#)
- 64 [“Electromagnetic Spectrum Superiority Strategy.”](#) DOD.
- 65 SSC Public Affairs, [“Space Systems Command Proves PTW SATCOM Capability for Warfighters to Operate More Effectively in Contested Environments.”](#) Space Systems Command, August 19, 2025.
- 66 Nesrine Benchoubane and Gunes Karabulut Kurt, [“Securing space domain awareness overview: decisions in the nick of time.”](#) *Nature Portfolio*, April 2, 2026.
- 67 [“Electromagnetic Spectrum Superiority Strategy.”](#) DOD.
- 68 Tereza Pultarova, [“Satellite jamming is a real and growing threat. How can we protect our space infrastructure?”](#) *Space.com*, April 7, 2025; [“Case Study: Viasat.”](#) ProtectNGO Foundation, June 2022.
- 69 Pultarova, [“Satellite jamming is a real and growing threat.”](#)
- 70 Lewis and Johnson, [“Accelerating 5G in the United States.”](#)
- 71 [“Spectrum at a Breaking Point: How Next-Gen Constellations Will Share, Compete, and Coexist in an Era of Explosive Demand.”](#) Panel Discussion, Space Symposium, April 16, 2026.



www.mitchellaerospacepower.org



