CSC 2.0

November 2026

Space Critical Infrastructure: The Final Frontier

How Congress Can Protect U.S. Space-Based Systems Amid Rising Threats

Emmerson Overell and Annie Fixler

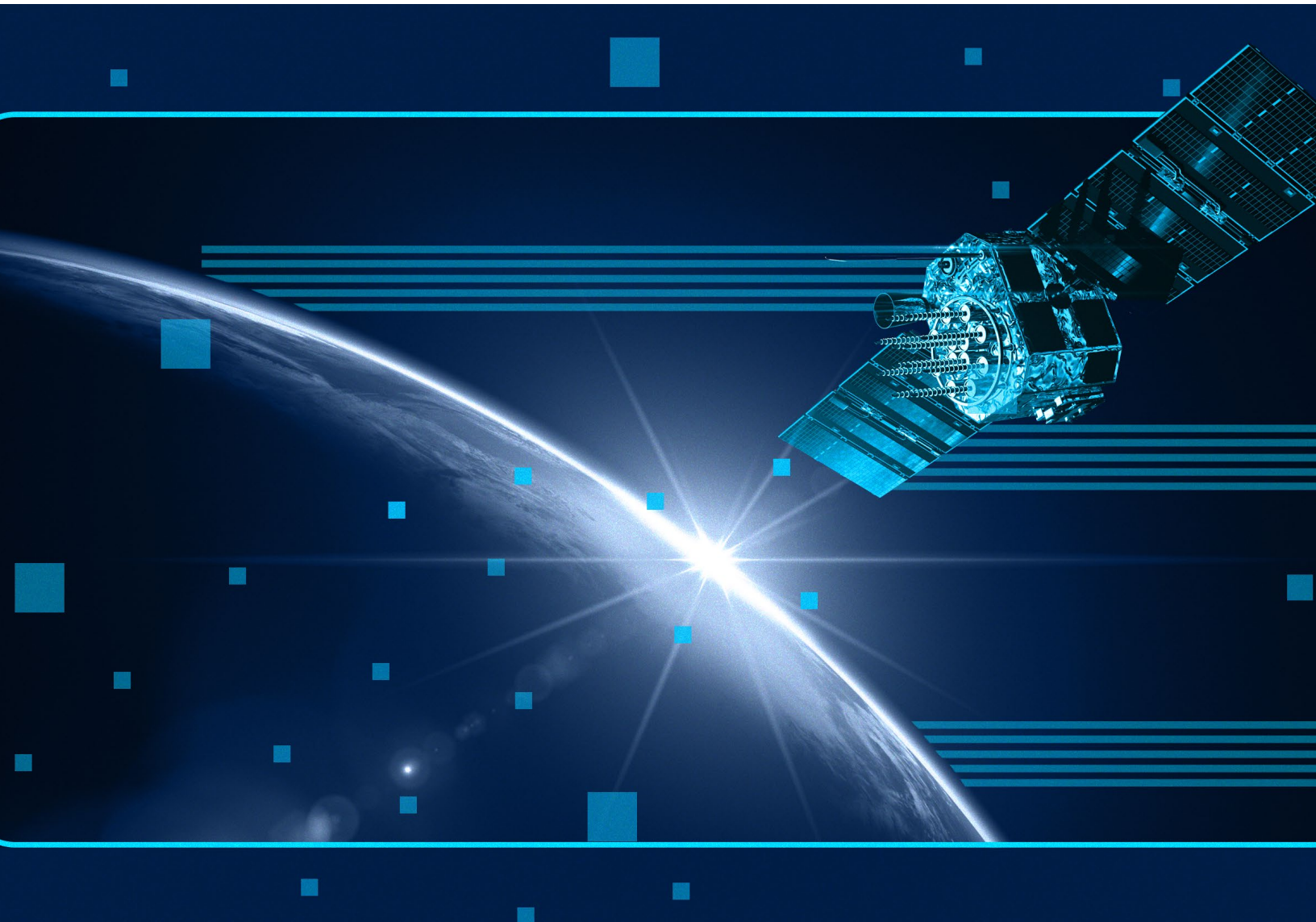


Table of Contents

Foreword **4**

Executive Summary **5**

The U.S. Space Ecosystem Is Growing More Commercial and More Interdependent **6**

Space Systems Already Function as Critical Infrastructure **8**

- Criticality of Space-Based Systems 8
- Disjointed Governance 9
- Failure To Launch 10

China and Russia Are Preparing To Disrupt U.S. Space Power **11**

- The People's Republic of China 12
- The Russian Federation 12
- Future Threats to Space-Based Assets 13

Recommendations: How Congress Should Designate Space-Based Systems as Critical Infrastructure **13**

Conclusion: Securing Space-Based Systems Means Securing American Daily Life **17**

Foreword

The United States has correctly designated the electric grid, financial system, and communications networks as sectors of critical infrastructure central to national security. But Washington has yet to address space infrastructure — upon which these and other critical infrastructure sectors increasingly depend — with the same urgency, prioritization, coherence, and clear lines of accountability.

This lack of action has become a major national security vulnerability.

For most of the space age, satellites were relatively few, expensive, and mainly launched and operated by governments. Space supported national power, but it remained separate from much of the infrastructure Americans encountered in their daily lives. That world is no longer.

Today, space systems are woven into the basic functioning of the U.S. economy, military operations, and American society. These systems connect forces across battlefields, synchronize computer networks, guide transportation, enable global communications, support financial transactions, control infrastructure operations, monitor weather, and provide imagery and other information that governments and businesses use every day to make decisions. The consequences of disruption would not remain confined to space. The loss or degradation of positioning, navigation, and timing; communications; or remote sensing could quickly cascade across telecommunications, energy, transportation, financial services, emergency response, and military operations.

This transformation has provided America with an extraordinary advantage. The United States leads a commercial space sector that is innovating at extraordinary speed and scale. U.S. military and intelligence agencies can draw on commercial communications, imagery, launch, and other services alongside government-owned capabilities. American leadership in space strengthens the economy while giving Washington options, capacity, and resilience that its adversaries will need to spend years or decades to replicate.

But dependence creates vulnerability. Much of the innovation, infrastructure, and operational capacity on which the nation increasingly depends is privately owned and operated. Government cannot secure this ecosystem alone; industry must be an operational partner in building its security and resilience.

China and Russia understand that they do not need to defeat the United States everywhere if they can disrupt the infrastructure that enables American power to function. Space-based systems are part of the connective tissue that allows both the military and the economy to operate. And the most consequential attack on a space system may not occur in space. Adversaries can launch cyber operations, generate electronic interference, compromise ground infrastructure, introduce supply-chain vulnerabilities, or attack commercial providers to disrupt space systems, all without launching a widely visible (and attributable) anti-satellite missile.

Washington therefore faces a policy mismatch. Space has evolved from a specialized capability into foundational infrastructure, while responsibility for its security remains fragmented across agencies, authorities, and the public and private sectors. The question is not simply whether Washington labels space as a critical infrastructure sector, but whether we organize, assign responsibility, build resilience, and operate the sector accordingly. Accountability must be clear and collaboration must become operational, not simply informational.

Three years ago, we argued that correcting this mismatch should be a priority for Congress and the executive branch.[1] Since then, America's dependence on space has deepened, commercial capabilities have expanded, and the threat environment has become far more contested. The gap between dependence and protection has therefore become more important, not less.

Critical infrastructure policy exists precisely so that we do not discover our dependencies only after an adversary exploits them. Congress has an opportunity to close this gap deliberately, before a crisis closes it for us. Protecting America's space infrastructure is no longer simply a space policy imperative. It is essential to protecting the nation's economic security, military power, and way of life.

RADM (Ret.) Mark Montgomery
Cyberspace Solarium Commission Executive Director

Frank Cilluffo
Distinguished Advisor to CSC 2.0

Executive Summary



An FDD design by Liz Sunshine featuring a satellite and sunrise in space (BlackJack3D via Getty Images).

Space is no longer a domain reserved for exploration, prestige, or military advantage. Space-based systems meet the functional definition of critical infrastructure: Their disruption or destruction would have cascading consequences for U.S. national security, economic security, public safety, and daily life. Yet Washington has failed to formally designate space systems as critical infrastructure, leaving the nation without a comprehensive framework to manage growing risks across the space ecosystem.

Satellites provide positioning, navigation, and timing (PNT) services that enable financial transactions, shipping, precision agriculture, and military operations. They support communications, weather forecasting, missile warning, intelligence collection, and logistics networks worldwide. In 2023, the Cyberspace Solarium Commission (CSC) 2.0 and McCrary Institute laid out the case for federal designation of space systems as critical infrastructure.[2] They concluded that while some systems are indirectly covered through existing sectoral designations, no single federal entity was responsible for assessing how risks to satellites, ground stations, launch systems, command-and-control links, space data services, and commercial providers interact as one interconnected system.

This incomplete coverage leaves gaps in U.S. defenses. Launch facilities, spacecraft and orbital constellations, ground stations, tracking and command systems, manufacturing facilities, and specialized space supply chains do not fit neatly within the risk-management plans of the communications, defense industrial base, or critical manufacturing sectors or those of the other sectors that rely on these assets. That leaves essential parts of the ground-to-orbit ecosystem without a risk framework.

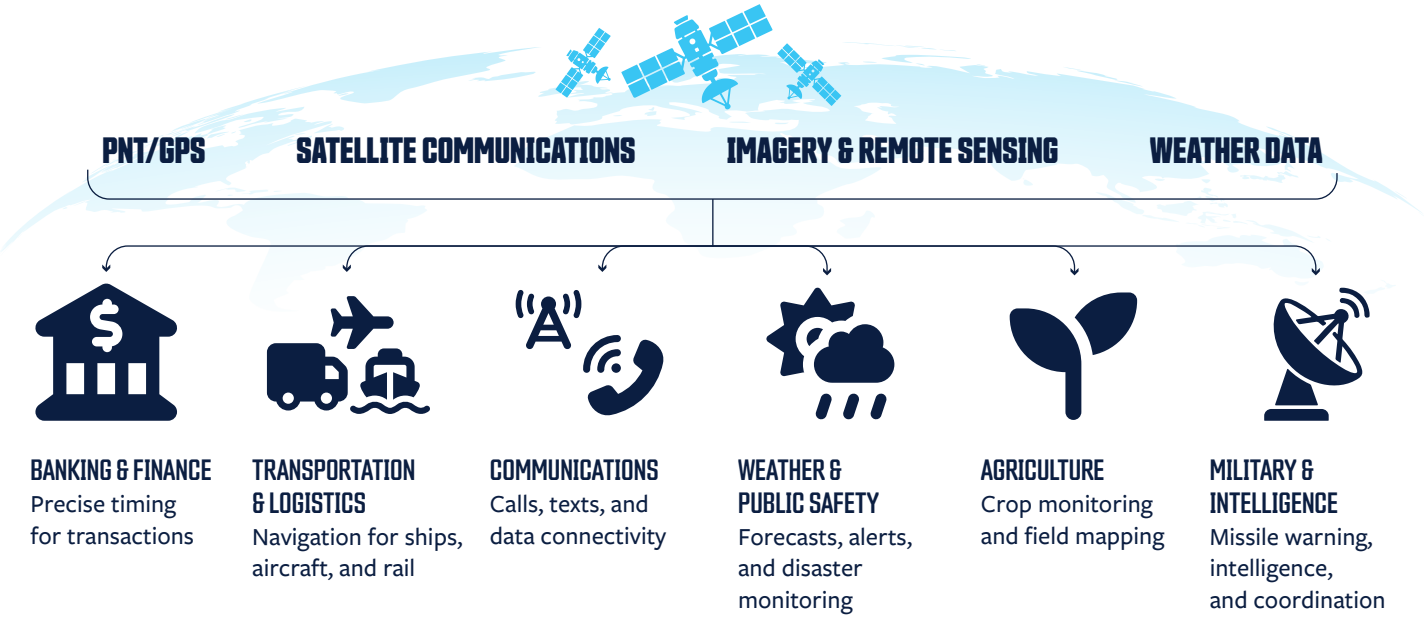
Three trends make this fragmented approach increasingly untenable. First, China and Russia are fielding counterspace capabilities to jam satellite communications, falsify navigation signals, maneuver near U.S. satellites to spy on them, or destroy satellites. The U.S. Space Force has repeatedly warned, "Intensifying strategic competition presents a serious threat to U.S. national security interests in, from, and to space."[3] In a crisis or conflict, U.S. adversaries could delay intelligence collection, disrupt command and control, degrade missile warning, and complicate offensive targeting.

Second, commercial providers' integration into federal and military space operations makes private-sector systems increasingly central to national security missions.[4]

Third, the American public, economy, and military increasingly depend on space-enabled services — including GPS navigation, timing for financial transactions, weather forecasting, and telecommunications. In 2022, Samuel Visner, board chairman of the Space Information Sharing and Analysis Center (Space ISAC), an industry-led threat-sharing organization, warned that "space systems are conceivably a target" for infrastructure attacks.[5] The growth of the industry's importance has only made it a more attractive target.

How Space Systems Support Daily Life and National Security

Space-based services underpin both civilian life and U.S. defense operations.



What has not changed is Washington's fragmented approach to managing those risks. The federal government recognizes 16 critical infrastructure sectors, each paired with a sector risk management agency (SRMA) as its day-to-day federal point of contact. Space has neither an SRMA nor a sector-specific risk management plan. No federal agency leads sector-wide efforts to help private space companies protect these interconnected systems.

Aligned with CSC 2.0's original assessment in 2023,[6] this report argues that Congress should designate space-based systems as the 17th critical infrastructure sector. Designation should neither create a new regulatory regime nor displace existing authorities. NASA should serve as the lead federal agency for sector-wide risk management, public-private collaboration, threat sharing, and resilience planning.

Since the 2023 report, technological, commercial, and international security changes have deepened space dependencies, but Washington still lacks the coordinating structure to manage them. Designation would help clarify federal responsibilities, strengthen commercial-federal coordination, improve cybersecurity and engineering resilience standards, and maintain reliable space services during crises or conflicts. In practice, American space architecture already functions as critical infrastructure. Congress should make that reality official.

The U.S. Space Ecosystem Is Growing More Commercial and More Interdependent

The American space ecosystem is no longer the government-led enterprise many still associate with the Cold War and Apollo era. It is increasingly commercial, distributed, and integrated into civilian life and national security operations. SpaceX, Blue Origin, commercial geospatial intelligence firms, satellite communications providers, launch companies, lunar logistics startups, and data providers are all shaping the future of U.S. space-enabled power.

The 2023 CSC 2.0 memo anticipated this transformation. It warned that arguments for preserving the existing governance framework would be "overtaken by events" as reusable launch systems, private space stations, commercial lunar operations, and other emerging activities expanded. Three years later, that forecast is being borne out.

The global space economy is projected to triple from $630 billion in 2023 to $1.8 trillion by 2035, according to a 2024 World Economic Forum report.[7] SpaceX began launching operational Starlink satellites in 2019, and by early 2026 had more than 10,000 active Starlink satellites in low-Earth orbit.[8]

Government-owned satellites remain essential, but commercial providers help fill gaps in coverage, capacity, speed, and resilience. Commercial satellite communications give military users more bandwidth, wider geographic reach, and backup pathways when government networks are unavailable, overloaded, or targeted by U.S. adversaries.[9] Commercial imagery and data providers supplement federal collection systems.[10] Commercial launch providers can expand access to orbit and increase the pace at which the United States can deploy, replace, or augment space systems.[11]

The Pentagon acknowledges the value of commercial capabilities. U.S. Space Force's vision for the next 15 years calls for augmenting future GPS with diverse allied and commercial navigation and timing systems, and envisions satellite communications built around a hybrid, self-healing architecture rather than small numbers of easily targeted satellites.[12] A self-healing network is resilient, designed to reroute data around jammed, degraded, or compromised components. The Defense Innovation Unit's Hybrid Space Architecture program seeks secure global internet connectivity across commercial, civil, military, allied, and partner systems in multiple orbits.[13] In plain terms, the Pentagon is trying to build an "outernet": a resilient space-based network that moves data across government, commercial, and allied systems rather than relying on a few satellites.[14]

Commercial providers are also increasingly embedded in sensitive military and intelligence missions. The National Reconnaissance Office (NRO) builds, launches, and operates U.S. spy satellites. In 2022, it awarded its largest-ever commercial imagery contracts to Maxar, Planet, and BlackSky through the Electro-Optical Commercial Layer Program, which supplies imagery to federal users.[15] NRO has also awarded commercial radio-frequency remote sensing study contracts to companies including Aurora Insight, HawkEye 360, Kleos Space, PredaSAR, Spire Global, and Umbra Lab.[16]

Reuters reported in 2024 that SpaceX's Starshield business unit was building a network of hundreds of spy satellites under a classified contract with the NRO.[17] NRO's Strategic Commercial Enhancements program pursues commercial sensing capabilities, including electro-optical, hyperspectral, radar, radio frequency, and lidar data.[18]

NASA also relies on commercial operators. The Artemis campaign relies on commercial partners for core mission components, including SpaceX and Blue Origin human landing systems.[19] NASA's Commercial Lunar Payload Services initiative uses American companies to deliver science, technology, and infrastructure payloads to the Moon. In November 2026, NASA selected eight companies, including Blue Origin, Firefly Aerospace, Intuitive Machines, and Voyager Technologies, for the next phase of the initiative.[20] The agency has also awarded Astrolab and Lunar Outpost task orders to build lunar terrain vehicles for Artemis astronauts, with Blue Origin selected for their planned delivery to the Moon in 2028.[21]

Allied and partner systems are becoming part of this architecture, too.[22] U.S. Space Command (SPACECOM) and close allies are developing a joint plan for defending orbital assets, while U.S. Space Force planning increasingly emphasizes allied and commercial systems as part of future resilience.[23] U.S. space architecture will increasingly combine federal, commercial, allied, and partner capabilities.

This commercial and allied dynamism is an American advantage, but the growing role of commercial and allied systems in government, military, intelligence, and critical civilian missions makes their security a national concern. Systems integrated into federal missions will become more attractive targets for cyberattacks, electronic warfare, software manipulation, supply-chain exploitation, and physical or orbital disruption. Growing U.S. dependence on commercial and partner space systems requires coherent federal governance to protect the interdependent ecosystem.

Space Systems Already Function as Critical Infrastructure

An industry's criticality depends not on its commercial value but on the consequences of its disruption. The U.S. government defines critical infrastructure as assets, systems, and networks whose incapacitation or destruction would have debilitating effects on security, the economy, public health, public safety, or some combination thereof.[24] By that standard, space-based systems already qualify. The Cybersecurity and Infrastructure Security Agency (CISA), the federal agency that coordinates critical infrastructure security and resilience, recognizes space systems' critical importance.[25] Washington has nevertheless not designated a space sector.

> ***"Since the late 1950s, space-enabled technologies have come to provide critical, yet often unrecognized, support to many of modern society's daily activities. Technological advancement and lower-cost barriers mean society is increasingly reliant on these technologies, and losing access to space-based services would have far-reaching effects."***
> *— Defense Intelligence Agency, Challenges to Security in Space*

Criticality of Space-Based Systems

Space supports other critical infrastructure sectors, including transportation, communications, finance, and agriculture. GPS does more than enable Google Maps or Waze to find a coffee shop or avoid traffic. Its PNT services route and track aircraft, ships, trucks, and trains and help emergency responders locate callers and dispatch personnel.[26] Financial institutions use precise satellite timing to maintain traceable records and verify when transactions occur down to the millisecond, supporting stock trades, bank transfers, and point-of-sale purchases.[27] Utilities use this same precise timing to synchronize the generation and transmission of electricity.28 Satellite links can extend phone and data services where ground networks are unavailable.[29] Agriculture uses satellite navigation, imagery, and weather data to monitor crops, map fields, and manage irrigation.[30] Weather satellites help forecasters track hurricanes, wildfires, floods, and severe storms so officials can prepare communities.[31] GPS, digital mapping, and remote sensing help responders map disaster areas, assess damage, guide emergency vehicles, and coordinate relief.[32]

Space-based systems support missile warning, intelligence collection, surveillance and reconnaissance, target identification, and tracking of adversarial activity.[33] American and allied forces rely on space-enabled services to see, communicate, move, evade, and defend.[34] Disruptions could hinder U.S. support for warfighters abroad and protection of citizens at home.

The U.S. Space Force's April 2026 Future Operating Environment 2040 assessment warned that even a single day without space-based services could disrupt weather alerts and emergency response, ground aircraft, reroute ships, and halt financial markets.[35] If the loss persisted for weeks or months, the assessment envisions shortages of fuel and hospital supplies, backed-up ports, disrupted rail schedules, missed agricultural harvesting windows, loss of power-grid synchronization, and slower cross-border financial activity.

The military consequences would be equally severe. The report warns that losing space services could reduce GPS-guided weapon accuracy, disrupt satellite-dependent command and control, shrink intelligence coverage, and slow strike- and joint-force coordination. Over time, degraded navigation and communications could slow military movements, increase the risk of forces mistakenly targeting one another, disrupt air defense and resupply operations, and weaken coordination with allies. In March 2026 House testimony, Gen. Stephen N. Whiting, commander of U.S. Space Command, similarly assessed that if an adversary degraded, denied, or destroyed U.S. space capabilities, the joint force's ability to fight as currently designed would be "immediately and materially impaired."[36]

Dependence on space-enabled services becomes a problem when no one federal agency is helping the industry understand the entire threat picture and mitigate risks. The Federal Aviation Administration (FAA), for example, helps aviation operators prepare for GPS interference,[37] but it does not protect the interconnected satellites, ground stations, command links, launch infrastructure, manufacturing base, and other systems that produce space services. Existing sectors' risk plans center on their own assets and missions rather than the full ground-to-orbit ecosystem. Space does not currently have dedicated sector-wide risk management.

Disjointed Governance

Space systems do not fit neatly into one vertical category like energy, transportation, or financial services. Instead, they operate horizontally across many of them. As a result, the governance of the sector is fragmented. Without designation as a critical infrastructure sector, space has no designated SRMA to coordinate agencies and operators, analyze sector risks, facilitate technical assistance and information sharing, and support incident management across the full ecosystem.[38]

NASA leads civil space exploration and scientific missions. The Department of Defense (DOD) oversees military space operations, while the intelligence community manages secretive national security space systems. The Federal Communications Commission (FCC) authorizes non-federal satellite systems and manages non-federal spectrum use, while the National Telecommunications and Information Administration (NTIA) manages federal spectrum, that is, radio frequencies used to transmit communications and data between satellites, ground stations, and users. The FAA licenses commercial launches, reentries, and spaceports. Meanwhile, the Department of Commerce licenses private remote-sensing systems and is developing civil space situational awareness and traffic coordination services.

CISA serves as the SRMA for the communications sector and the national coordinator for critical infrastructure security and resilience. It offers satellite communications operators cybersecurity guidance, assessments, and some information-sharing channels. Its Space Systems Critical Infrastructure Working Group brings government and industry partners together to develop risk-management strategies and cybersecurity recommendations.[39] Those efforts, however, are tied to existing critical infrastructure sectors, voluntary programs, and specific public-private partnerships. They do not amount to a comprehensive framework for managing risk across the entire space ecosystem.

Space ISAC enables government, industry, and academia to share threat information and coordinate responses to space vulnerabilities and incidents. Created in 2019, Space ISAC operates a Watch Center in Colorado Springs and is expanding its global network toward continuous threat monitoring.[40] As a private, member-driven organization, however, it cannot assign federal responsibilities, develop a government-wide sector risk plan, or lead an interagency response.

This division of responsibility creates both gaps and potential duplication. For example, a commercial satellite company supporting civilian and military customers may interact with the FCC over spectrum and satellite authorization; the FAA over launch; the Commerce Department over remote-sensing operations; the DOD or intelligence community over government contracts; Space ISAC over voluntary industry threat sharing; and CISA over voluntary cybersecurity support.

U.S. Space Governance is Fragmented

No single federal entity manages risk across the full space ecosystem

NASA
Civil space missions; proposed sector-wide coordinator

Department of Defense (U.S. Space Force)
Military space operations, situational awareness, and research

Department of Commerce (Office of Space Commerce, NTIA, NOAA)
Remote sensing, civil space situational awareness and traffic coordination, federal spectrum, commercial space business.

Space ISAC
Voluntary threat-sharing and watch center.

U.S. SPACE ECOSYSTEM

Intelligence Community (NRO)
National security space systems

FCC
Non-federal satellites and non-federal spectrum.

Department of Transportation (FAA)
Commercial launch, reentry, and spaceports

Department of Homeland Security (CISA)
National coordinator for critical infrastructure security and resilience; cybersecurity support.

WHY IT MATTERS

- Coordination and Security Gaps
- Overlap and Duplication
- Slower Incident Response

CURRENT GAP

Washington regulates and supports many parts of the space ecosystem, but no single entity manages sector-wide risk across satellites, ground stations, launch systems, command-and-control links, and space data services.

Each agency can address the part of the system within its authority, but none is responsible for mapping how a vulnerability in one part of the space systems sector — a satellite, ground station, command link, etc. — could cascade across the entire ecosystem. Nor is any one entity responsible for coordinating a sector-wide response when a disruption crosses several agencies' jurisdictions.

Consider a cyberattack on a commercial provider's ground network that disrupts military communications and civilian services. CISA would provide cybersecurity support, the FCC could address communications and spectrum, DOD could manage military consequences, and law enforcement or intelligence agencies could investigate. The response is likely to be disjointed, and the operator may face multiple reporting pathways and overlapping information requests.

This does not mean that existing agencies are failing. They are generally carrying out the missions Congress assigned them. Those mandates address specific functions — exploration, defense, spectrum, launch safety, or cybersecurity — rather than the resilience of interconnected civil, commercial, military, and intelligence space systems. Risks that fall between those individual mandates may not receive clear ownership, while lessons identified in one part of the ecosystem may not reach the others. For instance, a November 2026 Government Accountability Office report found that Space Force efforts to manage supply-chain risks were not sufficiently coordinated with other national security space stakeholders.41

Failure To Launch

Experts outside the U.S. government have argued for designation of space systems as critical infrastructure, and government officials have similarly recognized the criticality of space systems. When given the opportunity to address this reality, however, the federal government has punted.[42]

Space ISAC's Visner told Congress in April 2026 that "all critical infrastructures depend on space."[43] A 2025 Council on Foreign Relations task force recommended that the administration consider designating key space systems as critical infrastructure to provide a unified government contact for threat information, incident coordination, risk management, and recovery.[44]

In Congress, the case for action is slowly gaining bipartisan support. In February 2025, Reps. Ken Calvert (R-CA), Salud Carbajal (D-CA), Brian Fitzpatrick (R-PA), and Ted Lieu (D-CA) introduced the Space Infrastructure Act. The bill would direct the Department of Homeland Security (DHS) to designate space systems, services, and technology as a critical infrastructure sector, but it remains stalled before the House Science, Space, and Technology Committee.[45]

In September 2026, the Senate passed the bipartisan Satellite Cybersecurity Act of 2025, which awaits House action.[46] The bill would require the Department of Commerce, coordinating with DHS, to compile voluntary cybersecurity recommendations and maintain a public website with guidance and tools. It would also require a coordination strategy and a Government Accountability Office (GAO) review of federal support and critical infrastructure dependencies. Its provisions cover commercial satellites, supporting ground infrastructure, transmission links, and supply-chain risks.

Federal officials have acknowledged the importance of space systems but have not acted on this sentiment. Steve Casapulla, executive assistant director for the Infrastructure Security Division and interim assistant director for the National Risk Management Center at CISA, stated in April 2026, "Space-based assets are part of the nation's critical infrastructure and are increasingly integrated into daily life."[47]

Casapulla's comments echo an earlier report from CISA assessing the government's framework for critical infrastructure security. The November 2021 publication determined that space systems appeared to meet the threshold for designation as critical infrastructure, posing five questions that determine the necessary criteria:[48]

1. Does the scope describe a logical collection of assets, systems, or networks?
2. Does the scope provide common function to the economy, government, or society?
3. Could disruptions to the critical infrastructure sector lead to debilitating impacts on security, national economic security, national public health, or safety?
4. Is the critical infrastructure sector subject to risk drivers not fully addressed through existing mechanisms, policies, or governance structures?

5. Do key stakeholders within the critical infrastructure sector need to actively maintain their partnership beyond any existing collaboration mechanisms that may be in place?[49]

The White House committed in 2022 to "reviewing and revising" critical infrastructure sectors, but its April 2024 policy update retained the 16-sector structure without designating space.[50] A January 2025 Biden executive order recognized space systems' "pivotal role" in "critical infrastructure and communications resilience," but its space provisions applied only to federally owned or contracted systems.[51]

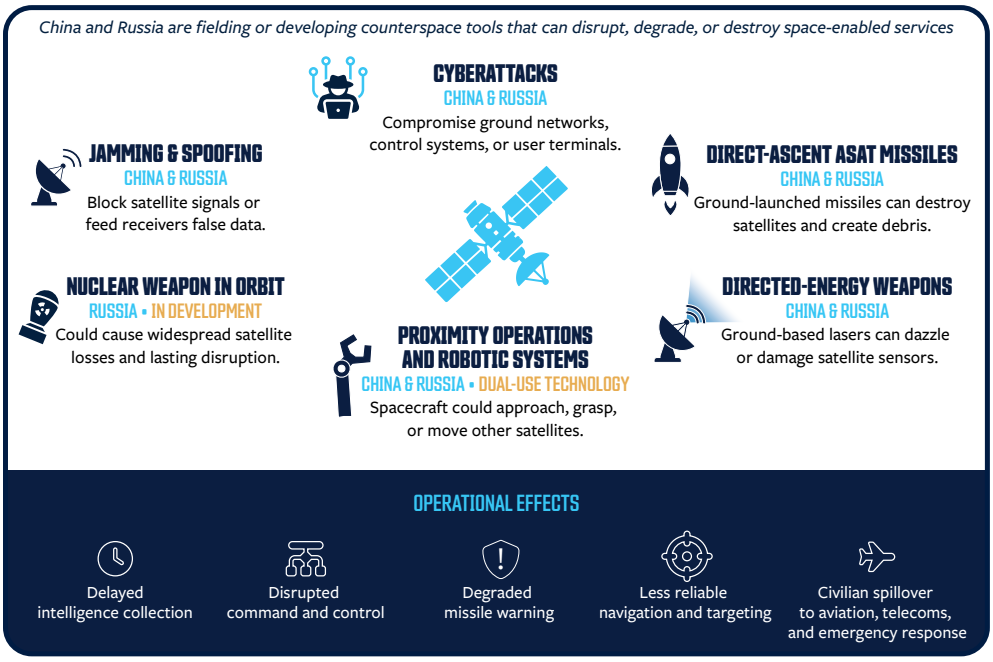
A January 2025 National Space Council and Office of the National Cyber Director report concluded that space systems "play an increasingly critical role for our national security, economy, and way of life" but that "holistic space cybersecurity practices are underdeveloped."[52] Industry representatives described guidelines as poorly suited to space systems and threat information as "inconsistent, untimely, not actionable."[53] The report documented industry concerns without establishing a federal implementation plan.

The Trump administration has prioritized American space superiority, but its initiatives remain focused on specific pieces of the problem — military space security, technological superiority, commercial growth, and launch infrastructure — rather than addressing the broader governance gaps surrounding the security and resilience of the full space ecosystem. A December 2025 executive order elevated both the economic and national security importance of space, directing the national security advisor to implement a space security strategy addressing current and projected threats to U.S. interests from very low-Earth orbit through cislunar space, the region between Earth and the moon.[54] The order also calls for a more responsive national security space architecture that integrates commercial capabilities and new market entrants.

The August 2026 National Security Science and Technology Strategy identifies space as a priority area for U.S. technological superiority, calls for capabilities to detect and counter threats from low-Earth orbit through cislunar space, and emphasizes technological resilience and redundancy.[55] The National Space Transportation Policy, released the same month, addresses launch infrastructure and industrial-base security and resilience, directing DOD and DHS to report on actions to secure launch infrastructure on federal property.[56] These policies strengthen important parts of space security but do not designate a space sector or assign an SRMA to coordinate its risks.

China and Russia Are Preparing To Disrupt U.S. Space Power

Rising threats to U.S. Space Systems



"China is the PACING CHALLENGE and is rapidly improving its space capabilities to TRACK & TARGET U.S. military forces. China & Russia are pursuing a wide range of counterspace capabilities to DISRUPT & DEGRADE U.S. space capabilities."

— United States Space Force, Space Threat Fact Sheet

In 2023, CSC 2.0 warned that China and Russia possessed or were developing anti-satellite missiles, cyber capabilities, jammers, lasers, and spacecraft that could interfere with other satellites.[57] It cited Russia's 2022 attack on U.S. satellite communications company Viasat, attempts to jam SpaceX's Starlink, and Chinese weapons intended to "blind and deafen" adversaries. Since 2023, these threats have grown in scale and sophistication.

The People's Republic of China

Beijing aims to exploit the U.S. military's dependence on space. SPACECOM reported in March 2026 that China operated more than 500 intelligence, surveillance, and reconnaissance satellites.[58] These systems help the People's Liberation Army track and target U.S. and allied forces with long-range precision weapons.

DOD's 2025 China Military Power Report states that Beijing is developing counterspace capabilities to deny U.S. forces access to satellite services during conflict.[59] These include missiles that destroy satellites and tools that interfere with their signals, sensors, and control networks.

The Pentagon also assesses that Chinese cyber actors infiltrate U.S. space and defense networks, likely for intelligence collection and operational preparation of the battlefield, which refers to establishing access for cyberattacks during a future conflict. China fields ground-based jammers and is developing systems to interfere with satellite communications, navigation, and radar imagery. It has also deployed ground-based lasers that could disrupt or damage satellites.[60] In practical terms, these attacks could cut military communications, feed false navigation data to ships or aircraft, obstruct satellite imagery, or compromise ground networks controlling spacecraft. Early in a conflict, they could delay U.S. decisions and hinder deployments and operations.[61]

Beijing is demonstrating more sophisticated behavior in orbit as well. In 2024, five Chinese experimental spacecraft maneuvered close to one another in coordinated patterns, which a senior Space Force official later described as "dogfighting in space."[62] These maneuvers demonstrated skills China could use to position its satellites for coordinated attacks on U.S. spacecraft during a conflict.[63]

The Pentagon also reports that Chinese satellites have repeatedly approached foreign spacecraft. In January 2022, Shijian-21 towed China's own defunct BeiDou-2 G2 navigation satellite into a higher orbit used for retired satellites.[64] Such servicing technology could be used to move U.S. satellites and disrupt their operations.[65] China's 2025 docking and refueling capabilities, meanwhile, could allow its spacecraft to sustain operations against U.S. satellites for longer.[66]

The Russian Federation

Four years ago, Russia demonstrated how counterspace operations can produce effects on Earth. Roughly an hour before invading Ukraine on February 24, 2022, Russia attacked Viasat's KA-SAT network, which provided satellite internet across Europe, including Ukraine. British officials believed the Ukrainian military was the primary target.[67] Attackers exploited faulty settings in ground equipment to access the network's management system and disable tens of thousands of customer modems, cutting internet access in parts of Ukraine and broader Europe.[68]

Russia later warned in October 2022 at the United Nations that commercial satellites supporting military operations could become legitimate targets for retaliation.[69] Fast forward to July 2026 and Russia is putting this policy into action, deploying powerful electronic warfare systems to interfere with Starlink connections used to control Ukrainian drones.[70]

Russian interference has also affected civilian navigation. SPACECOM reported that Moscow's continued jamming of GPS and other satellite navigation signals around the Baltic, Black Sea, and Mediterranean regions in 2025 caused flight diversions and reduced navigation accuracy.[71] "Jamming" blocks navigation signals, while "spoofing" tricks receivers with false position or timing data. Such interference can force pilots to rely on backup navigation, reroute or divert flights, and respond to false cockpit warnings.[72]

Directly destructive counterspace weapons also remain a serious threat. In 2021, Russia destroyed one of its own defunct satellites with a ground-launched anti-satellite missile, creating more than 1,500 trackable debris pieces and likely hundreds of thousands of smaller fragments.[73] U.S. officials warned that the debris could endanger satellites, space missions, and human spaceflight for years.[74] In March 2026, SPACECOM warned that Moscow was developing a nuclear anti-satellite weapon for placement in orbit and that a detonation could destroy thousands of satellites and leave low-Earth orbit unusable for years.[75]

Future Threats to Space-Based Assets

China and Russia view space as an operational domain where U.S. advantages can be weakened before or during conflict. SPACECOM warned Congress in March 2026 that threats across ground infrastructure, orbit, and cyberspace are no longer future possibilities but current operational realities.[76]

During a crisis or conflict, cyberattacks, signal jamming, or physical attacks on space systems could delay intelligence collection, disrupt military coordination, weaken missile warning, and make navigation and targeting less reliable. Deliberate interference may initially appear accidental, delaying recognition of an attack and identification of the attacker. That uncertainty could complicate a U.S. response.[77] Because many of the same commercial and government systems also support aviation, telecommunications, emergency response, and other civilian functions, the consequences could quickly spread beyond the military.[78]

Moreover, the counterspace capabilities China and Russia are fielding today may continue to grow in sophistication. The U.S. Space Force's 2040 assessment anticipates a future operating environment shaped by persistent cyber operations, electronic interference, deceptive signals, autonomous systems, and attacks that move rapidly between jamming, spoofing, cyber manipulation, physical disablement, and destructive effects.[79] It warns that both military and civilian space infrastructure could become targets, and that commercial operators and neutral countries could be drawn into conflict because the same systems increasingly support military and civilian users.

Looking ahead, the most damaging scenario may not be kinetic attacks on satellites, but a prolonged campaign of difficult-to-attribute interference that gradually reduces confidence in American navigation, communications, imagery, and warning data. The threats identified in 2023 have not disappeared; the U.S. Space Force now expects them to converge into persistent, integrated campaigns that simultaneously affect military, civilian, commercial, and allied systems.

Recommendations: How Congress Should Designate Space-Based Systems as Critical Infrastructure

Congress should designate space-based systems as the 17th critical infrastructure sector and NASA as its non-regulatory SRMA. NASA should coordinate risk management across government and industry, while other SRMAs that oversee components of the space ecosystem retain their authorities.

Designation alone, however, will not close the governance gaps identified above. Congress should require NASA to develop a sector-specific risk management plan, establish functional subgroups, coordinate cybersecurity and operational resilience baselines for systems supporting critical missions, and lead regular degraded-operations exercises with government and industry.

Together, these steps would clarify responsibilities, expose cross-sector dependencies, improve information sharing, and prepare the United States to sustain essential space-enabled services during crisis or conflict.

1. Congress should designate space-based systems as the 17th critical infrastructure sector.

Congress should define space-based systems broadly to encompass the full ground-to-orbit ecosystem. CSC 2.0 defined space systems as extending from ground to orbit, including sensors and signals, data and payloads, critical technologies, and supply chains. That broad definition is necessary because space risk does not stop at the satellite. Disruptions to ground stations, command links, or user terminals can interrupt essential services even when satellites remain in orbit.

At minimum, the sector should include:

- Satellites and spacecraft
- Ground stations and mission operations centers
- Telemetry, tracking, and command systems
- Launch-related systems

- Satellite communications systems and user terminals
- PNT services
- Space-based data services, including remote sensing and weather data
- Mission software and cloud-based space data infrastructure
- Space hardware, software, and component supply chains
- Commercial systems supporting critical civilian or national security functions

A broader sector definition would allow the government to assess space risk as a system-of-systems problem rather than as a set of disconnected assets.

2. Congress should designate NASA as the non-regulatory SRMA.

Congress should designate NASA as the SRMA for the space systems sector. NASA is the best-positioned federal entity for this role because space is its core institutional mission. Other agencies engage with space through narrower responsibilities: DOD and the intelligence community through national security missions; the FCC and NTIA through spectrum and communications; the FAA through launch and reentry safety; Commerce through remote sensing and space traffic coordination; and CISA through cybersecurity and critical infrastructure. NASA, by contrast, has decades of experience designing, operating, evaluating, and managing complex space systems across the civil-commercial boundary.

NASA combines space engineering and mission-assurance expertise — the work of keeping missions safe and reliable — with longstanding commercial partnerships.[80] Its work on crew transportation, lunar deliveries, human landing systems, and other missions requires setting technical requirements, evaluating risk, and coordinating with government and industry partners.[81] After interviewing more than 30 government and industry experts in 2023, CSC 2.0 identified NASA as the strongest candidate for SRMA.

Congress should also affirm what would remain outside NASA's remit. As SRMA, NASA would not become the regulator of the U.S. space economy. Instead, NASA would coordinate sector-wide risk management, public-private collaboration, threat sharing, resilience planning, and congressional reporting. NASA's role would be to connect existing operational and regulatory functions, not replace them. All other federal entities with space-related authorities would keep their existing roles, and NASA would help align those efforts within a sector-wide risk management framework. This structure should offer industry a clear value proposition: better threat sharing, clearer federal points of contact, stronger resilience planning, and greater support during crises — not additional regulation.

However, NASA is not currently structured or resourced to secure the entire U.S. space ecosystem. Its security and mission-assurance responsibilities have historically centered on NASA missions rather than sector-wide risk. To support NASA as non-regulatory SRMA, Congress should provide dedicated funding and staff so that NASA would not have to divert resources from its existing civil exploration missions.

CSC 2.0 therefore recommended an initial investment of $15 million per year to support 25 full-time employees for NASA's SRMA responsibilities. Congress should use that figure as the starting point, while directing the Office of Management and Budget and NASA to reassess future needs as the sector matures. When hiring staff to support SRMA duties, NASA should prioritize expertise in space engineering, cybersecurity, mission reliability, industry engagement, incident and interagency coordination, supply chains, and dependency mapping.

3. Congress should require NASA to develop a sector-specific risk management plan.

Congress should require NASA to publish a sector-specific risk management plan within one year of designation. The plan should define the sector, identify key dependencies, map critical nodes, assess cyber and engineering risks, evaluate supply-chain vulnerabilities, identify commercial-federal dependencies, and propose priority areas for public-private collaboration.

The plan should also map existing reporting and coordination pathways so that NASA does not duplicate these efforts. Mechanisms already exist, including industry threat-sharing through Space ISAC, CISA's work with public and private partners on space system security and resilience, and FCC-NTIA coordination on spectrum issues. NASA should identify where existing pathways are sufficient, where they overlap, and where there are gaps that could hinder responses to incidents that cut across civil, commercial, military, intelligence, cyber, and communications equities.

This mapping should produce clear escalation procedures for space-related disruptions. If a commercial satellite operator experiences cyber interference, ground-network intrusions, jammed communications, or false navigation signals, operators should know whom to notify, how information is shared across the government, and which agency leads the response.

Additionally, the plan should include degraded-operations planning. NASA, working with the DOD, intelligence community, DHS, and other relevant entities, should assess how federal agencies and critical infrastructure operators would function if key space-enabled services were disrupted or unavailable. A "space zero day" scenario would represent a sudden, significant loss or compromise of space-enabled services before agencies, operators, or the public fully understand the cause or scope of the disruption. Planning for the worst-case scenario would help Washington identify which services must be restored first, what backup capabilities exist, and how stakeholders would communicate during such an incident.

4. Congress should direct NASA to establish space-sector subgroups.

Congress should direct NASA to establish functional subgroups within the space systems sector. The sector spans national security satellites, commercial communications networks, civil missions, and the ground systems and services supporting them. These activities have different security needs, operating requirements, and federal authorities that a single centralized process would struggle to address. Subgroups would bring together the relevant agencies and operators to manage those differences while NASA coordinates risks across the sector.

Each subgroup should identify risks, map dependencies on other space and terrestrial systems, set resilience priorities, and coordinate incident response planning. Their recommendations should inform NASA's broader sector risk management plan, helping the agency understand how disruptions could spread across systems.

Existing agencies would retain their responsibilities: DOD and the intelligence community for national security space systems; the FCC and NTIA for spectrum; and CISA for communications infrastructure. NASA would draw on their expertise and coordinate their contributions to the sector plan.

NASA could use the proposed subgroups below as a general baseline:

- National Security Space Subgroup: Focusing on defense, intelligence, missile warning, sensitive communications, and related space systems, this subgroup should include DOD, NTIA, DHS, intelligence community agencies, and other relevant entities. The National Reconnaissance Office should coordinate intelligence-community participation in the subgroup, while DOD should coordinate military-space equities.
- Commercial and Civil Space Subgroup: Focusing on commercial launch, civil space missions, data services, ground infrastructure, software, emerging space operators, and other relevant parties, this subgroup should include the Departments of Commerce and Transportation, FCC, DHS, NASA, and other relevant entities. Its purpose would be to identify risks affecting commercial and civil systems and improve public-private coordination.
- Communications Subgroup: Focusing on satellite communications, spectrum-dependent services, command-and-control links, PNT dependencies, and communications continuity, this subgroup should include the FCC, FAA, NTIA, DOD, DHS, NASA, Commerce, industry representatives, and other relevant parties. The FCC, NTIA, and CISA would retain their respective regulatory, spectrum-management, and critical infrastructure risk-management roles.

These subgroups would give NASA a practical governance structure for identifying vulnerabilities, prioritizing resilience investments, coordinating with industry, and preparing for disruptions that could affect both national security and civilian life. To ensure that these subgroups sufficiently address the cross-sector interests in space, Congress should task the GAO with assessing all the federal entities that have authorities or interests in the space ecosystem.

5. Congress should standardize space-sector cybersecurity and operational resilience requirements for systems supporting critical missions.

Congress should direct NASA to lead the development of space-sector cybersecurity and operational resilience standards for federal and commercial space systems that support critical functions or national security missions. NASA should develop this profile in coordination with DHS, Commerce, DOD, other relevant federal entities, and commercial operators.

NASA should align existing cybersecurity frameworks and contractor requirements, not duplicate or replace them. Federal contractors already face information security requirements, including obligations tied to protecting controlled unclassified

information and meeting DOD cybersecurity expectations. Existing frameworks also provide useful cyber risk management tools. But these standards do not yet provide a unified, space-sector-specific framework focused on operational resilience across the full space mission chain.

The space-sector cybersecurity standards should identify where existing cybersecurity requirements are sufficient, where they are duplicative or redundant, and where additional mission-assurance expectations are needed. The latter should focus on whether systems can continue operating, fail safely, or recover quickly during cyber, electronic, or operational disruption.

At minimum, the standards should address:

- Secure telemetry, tracking, and command systems
- Authentication and access controls for mission-critical systems
- Encryption for sensitive command, control, and data links
- Software and firmware integrity
- Secure update mechanisms
- Logging and anomaly detection for satellite and ground systems
- Incident reporting pathways for space-related disruptions
- Supply-chain risk management for space hardware, software, and components
- Backup PNT options
- Degraded-mode functionality
- Redundant communications pathways
- Recovery timelines for critical services
- Public messaging and assistance during disruptions
- Resilience-by-design engineering principles

Federal customers, including DOD, the intelligence community, and NASA, should review existing contract requirements against the developed baseline and address gaps in future procurements. Applicable provisions should include testing to verify that purchased systems can protect essential services and recover from disruption. For operators outside federal contracting, NASA and CISA should support voluntary adoption through technical assistance and exercises. Rather than turning NASA into a regulator, the standards should establish a shared resilience baseline for space systems supporting critical functions.

6. Congress should require joint space zero day wargaming and degraded-operations exercises across government and industry.

Congress should require all relevant federal agencies to conduct regular space zero day exercises with commercial operators that provide broad public services and space-related government contractors. These exercises should test scenarios in which key space-enabled services are disrupted, degraded, spoofed, jammed, or temporarily unavailable.

DOD is already leading the way. SPACECOM has launched commercial wargames involving industry participants to examine hard problems in orbit, including threats related to weapons of mass destruction in space.[82] The U.S. Space Force also has doctrine and wargaming units designed to prepare Guardians — Space Force members — for contested space operations.[83] These critical efforts should be expanded.

Current efforts, however, remain largely centered on military space operations and industry participation in national security missions. The 2020 National Space Policy called for simulating space disruptions in interagency and national exercises.[84] Congress should build on this direction and existing military exercises by requiring a sustained whole-of-government exercise program — potentially as part of the National Exercise Program. These exercises should test both military operations and civilian consequences, including backup position-navigation-timing, communications alternatives, commercial continuity, public messaging, allied coordination, emergency response, and cross-agency decision-making. If civilian life and military power depend on space systems, then Washington should regularly practice what happens when those systems are degraded or unavailable.

Conclusion: Securing Space-Based Systems Means Securing American Daily Life

Space security is no longer separate from terrestrial security. It is the infrastructure layer that enables modern finance, communications, transportation, agriculture, weather forecasting, intelligence collection, missile warning, and critical military operations.

America's adversaries understand this, which is why they are developing capabilities to disrupt, degrade, and destroy the space-based systems that give the United States its potent military, intelligence, and economic advantages. Designating space systems as the 17th critical infrastructure sector, naming NASA as the SRMA, and establishing the sector-wide risk management, resilience, and exercise framework outlined above would help protect these advantages.

Congress should address this challenge now rather than wait for a major disruption to space systems. Technologies and strategic trends are converging toward a space environment fundamentally different from today's.[85] Planning and investment decisions made now will shape whether the United States is prepared for the new age of space. Technological superiority alone will be insufficient, but the organization, integration, and clarity of strategic purpose will be decisive. To protect America's livelihoods and prosperity on Earth, the United States must secure the systems above it.

Endnotes

1. Frank Cilluffo, Mark Montgomery, Sharon Cardash, and Kelsey Shields, "Time to Designate Space Systems as Critical Infrastructure," *CSC 2.0*, April 14, 2023. (https://cybersolarium.org/csc-2-0-reports/time-to-designate-space-systems-as-critical-infrastructure)

2. Ibid.

3. "Space Threat Fact Sheet," *U.S. Space Force*, accessed October 21, 2026. (https://www.spaceforce.mil/About-Us/Fact-Sheets/Fact-Sheet-Display/Article/4297159/space-threat-fact-sheet)

4. Chief of Space Operations Gen. Chance Saltzman, "Remarks by CSO Gen. Chance Saltzman at the 2026 Space Symposium," *Remarks at the 41st Space Symposium*, April 15, 2026. (https://www.spaceforce.mil/News/Article-Display/Article/4461041/remarks-by-cso-gen-chance-saltzman-at-the-2026-space-symposium)

5. Debra Werner, "Russian invasion of Ukraine exposes cybersecurity threat to commercial satellites," *SpaceNews*, April 14, 2022. (https://spacenews.com/russian-invasion-of-ukraine-exposes-cybersecurity-threat-to-commercial-satellites)

6. Frank Cilluffo, Mark Montgomery, Sharon Cardash, and Kelsey Shields, "Time to Designate Space Systems as Critical Infrastructure," *CSC 2.0*, April 14, 2023. (https://cybersolarium.org/csc-2-0-reports/time-to-designate-space-systems-as-critical-infrastructure)

7. "Space: The $1.8 Trillion Opportunity for Global Economic Growth," *World Economic Forum*, April 8, 2024. (https://www.weforum.org/publications/space-the-1-8-trillion-opportunity-for-global-economic-growth)

8. Robert Z. Pearlman, "SpaceX launches 10,000th active Starlink satellite in low Earth orbit (video)," *Space.com*, March 17, 2026. (https://www.space.com/space-exploration/launches-spacecraft/spacex-launches-10-000th-active-starlink-satellite-into-low-earth-orbit)

9. Theresa Hitchens, "Into the 'outernet': Secure 'internet in space' key to future Space Force hybrid architecture," *Breaking Defense*, July 14, 2022. (https://breakingdefense.com/2022/07/into-the-outernet-secure-internet-in-space-key-to-future-space-force-hybrid-architecture); Defense Innovation Unit, "Hybrid Space Communications Network Leverages Commercial Technology, Enabling Faster Decision-Making on the Battlefield," accessed September 3, 2026. (https://www.diu.mil/latest/hybrid-space-communications-network-leverages-commercial-technology-enabling); Defense Innovation Unit, "Initial contracts for Hybrid Space Architecture Program," July 7, 2022. (https://www.diu.mil/latest/developing-the-internet-of-space)

10. National Reconnaissance Office, Press Release, "NRO announces largest award of commercial imagery contracts," May 25, 2022. (https://www.nro.gov/Portals/135/documents/news/press/2022/press_release_05-22.pdf)

11. U.S. Space Force Space Systems Command, Press Release, "US Space Force demonstrates responsive launch for VICTUS HAZE mission, begins on-orbit operations," June 22, 2026. (https://www.ssc.spaceforce.mil/Newsroom/Article-Display/Article/4523601/us-space-force-demonstrates-responsive-launch-for-victus-haze-mission-begins-on); Michael O'Connor and Kathleen Curlee, "Shaping the U.S. Space Launch Market: Extending America's Advantage," *Center for Security and Emerging Technology*, February 2025, page 1. (https://cset.georgetown.edu/wp-content/uploads/CSET-Shaping-the-U.S.-Space-Launch-Market.pdf)

12. U.S. Space Force, "Objective Force 2040," April 2026. (https://www.spaceforce.mil/Portals/2/Documents/SAF_2026/OFD_2040_Baseline_Final.pdf); U.S. Space Force, "CSO debuts Future Operating Environment, Objective Force at 41st Space Symposium," April 15, 2026. (https://www.spaceforce.mil/News/Article-Display/Article/4461061/cso-debuts-future-operating-environment-objective-force-at-41st-space-symposium)

13. Defense Innovation Unit, "Initial contracts for Hybrid Space Architecture Program," July 7, 2022. (https://www.diu.mil/latest/developing-the-internet-of-space)

14. Emmerson Overell, "The Pentagon Is Transforming U.S. Commercial Satellites Into Tactical Battlefield Infrastructure," *Foundation for Defense of Democracies*, May 14, 2026. (https://www.fdd.org/analysis/2026/05/14/the-pentagon-is-transforming-u-s-commercial-satellites-into-tactical-battlefield-infrastructure)

15. National Reconnaissance Office, Press Release, "NRO announces largest award of commercial imagery contracts," May 25, 2022. (https://www.nro.gov/Portals/135/documents/news/press/2022/press_release_05-22.pdf)

16. National Reconnaissance Office, Press Release, "NRO Announces Commercial Radio Frequency Study Contract Awards," September 28, 2022. (https://www.nro.gov/news-media-featured-stories/news-media-archive/News-Article/Article/3173098/nro-announces-commercial-radio-frequency-study-contract-awards)

17. Joey Roulette and Marisa Taylor, "Musk's SpaceX is building spy satellite network for U.S. intelligence agency, sources say," *Reuters*, March 16, 2024. (https://www.reuters.com/technology/space/musks-spacex-is-building-spy-satellite-network-us-intelligence-agency-sources-2024-03-16)

18. National Reconnaissance Office, "Maj. Gen. Povak Speaks at NSSA DISC; Announces Latest Commercial Contracts," February 12, 2026. (https://www.nro.gov/news-media-featured-stories/news-media-archive/News-Article/Article/4405778/maj-gen-povak-speaks-at-nssa-disc-announces-latest-commercial-contracts)

19. National Aeronautics and Space Administration, Press Release, "NASA Awards Moon Base Transportation, Technology, Science Projects," November 7, 2026. (https://www.nasa.gov/news-release/nasa-awards-moon-base-transportation-technology-science-projects); NASA, Partners Accelerate Lander Development for 2028 Moon Missions," *National Aeronautics and Space Administration*, October 23, 2026. (https://www.nasa.gov/missions/artemis/nasa-partners-accelerate-lander-development-for-2028-moon-missions)

20. National Aeronautics and Space Administration, Press Release, "NASA Awards Moon Base Transportation, Technology, Science Projects," November 7, 2026. (https://www.nasa.gov/news-release/nasa-awards-moon-base-transportation-technology-science-projects)

21. National Aeronautics and Space Administration, Press Release, "NASA Provides Update on Moon Base Rovers, Landers, Missions," May 26, 2026. (https://www.nasa.gov/news-release/nasa-provides-update-on-moon-base-rovers-landers-missions); Victoria Ugalde, "NASA Provides Progress Update on Moon Base Rovers," *National Aeronautics and Space Administration*, October 20, 2026. (https://www.nasa.gov/missions/moon-base/nasa-provides-progress-update-on-moon-base-rovers)

22. Theresa Hitchens, "US, close allies creating joint 'orbital warfare' plan: SPACECOM chief," *Breaking Defense*, May 12, 2026. (https://breakingdefense.com/2026/05/us-close-allies-creating-joint-orbital-warfare-plan-spacecom-chief)

23. Courtney Albon, "US Space Command, Allies Crafting Ops Plan for Orbital Warfare," *Air & Space Forces Magazine*, May 13, 2026. (https://www.airandspaceforces.com/us-space-command-allies-ops-plan-orbital-warfare); U.S. Space Force, "Objective Force 2040," April 2026. (https://www.spaceforce.mil/Portals/2/Documents/SAF_2026/OFD_2040_Baseline_Final.pdf)

24. U.S. Defense Intelligence Agency, "Challenges to Security in Space 2022," accessed October 29, 2026. (https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf); "Critical Infrastructure Sectors," *Cybersecurity and Infrastructure Security Agency*, accessed September 3, 2026. (https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors)

25. Cybersecurity and Infrastructure Security Agency, "FY 2021 National Defense Authorization Act: Section 9002(b) Report," November 12, 2021, page 44. (https://www.cisa.gov/sites/default/files/2023-01/Section_9002_NDAA_Report_FINAL_508c.pdf)

26. U.S. Government Accountability Office, "GPS Disruptions: DOT Could Improve Efforts to Identify Interference Incidents and Strengthen Resilience," December 15, 2022, pages 5-6. (https://www.gao.gov/assets/gao-23-105335.pdf); "Public Safety & Disaster Relief," *U.S. Space Force*, accessed October 25, 2026. (https://archive.gps.gov/applications/safety)

27. "GPS and Financial Institutions," *U.S. Space Force*, accessed September 3, 2026. (https://www.gps.gov/gps-and-financial-institutions); Lisa Sodders, "50 Years Later, the Atomic Clocks on GPS Satellites Continue to Keep the World in Sync," *U.S. Space Force Space Systems Command*, January 15, 2024. (https://www.ssc.spaceforce.mil/Newsroom/Article/4039094/50-years-later-the-atomic-clocks-on-gps-satellites-continue-to-keep-the-world-i)

28. Marc A. Weiss, Alison Silverstein, Francis Tuffner, and Ya-Shian Li-Baboud, "The Use and Challenges of Precise Time in Electric Power Synchrophasor Systems," *National Institute of Standards and Technology*, January 30, 2017. (https://www.nist.gov/publications/use-and-challenges-precise-time-electric-power-synchrophasor-systems)

29. Single Network Future: Supplemental Coverage From Space; Space Innovation, Federal Communications Commission, 89 Federal Register 34148, April 30, 2024, paragraphs 1 and 8. (https://www.federalregister.gov/d/2024-06669)

30. "Precision Agriculture with GPS," U.S. Space Force, accessed October 25, 2026. (https://www.gps.gov/precision-agriculture-gps); "Agriculture," *National Aeronautics and Space Administration*, accessed October 25, 2026. (https://mynasadata.larc.nasa.gov/basic-page/agriculture)

31. National Oceanic and Atmospheric Administration, "5 Ways NOAA's Satellites Support Emergency Managers and First Responders," April 20, 2026. (https://www.nesdis.noaa.gov/news/5-ways-noaas-satellites-support-emergency-managers-and-first-responders)

32. "Public Safety & Disaster Relief," *U.S. Space Force*, accessed October 25, 2026. (https://archive.gps.gov/applications/safety)

33. Bruce Berkowitz and Michael Suk, "The National Reconnaissance Office at 50 Years: A Brief History," *Center for the Study of National Reconnaissance*, July 2018. (https://www.nro.gov/Portals/135/documents/about/50thanniv/The%20NRO%20at%2050%20Years%20-%20A%20Brief%20History%20-%20Second%20Edition.pdf)

34. Joanne Swann, "Why Modern Military Power Depends on Space," *Defence iQ*, accessed September 3, 2026. (https://www.defenceiq.com/isr/articles/why-modern-military-power-depends-on-space)

35. U.S. Space Force, "Future Operating Environment 2040," April 2026. (https://www.spaceforce.mil/Portals/2/Documents/SAF_2026/Future_Operating_Environment_2040_Final.pdf)

36. Commander of U.S. Space Command Gen. Stephen N. Whiting, "Fiscal Year 2027 Priorities and Posture of United States Space Command," *Testimony before the House Armed Services Committee, Subcommittee on Strategic Forces*, March 17, 2026. (https://www.spacecom.mil/Portals/57/2026%20CDRUSSPACECOM%20Posture%20Statement%20-%20Final.pdf)

37. Federal Aviation Administration, "Global Navigation Satellite System (GNSS) Interference Resource Guide," accessed October 25, 2026. (https://www.faa.gov/about/office_org/headquarters_offices/avs/offices/afx/afs/afs400/afs410/GNSS)

38. "Sector Risk Management Agencies," *Cybersecurity and Infrastructure Security Agency*, accessed September 3, 2026. (https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/sector-risk-management-agencies)

39. "Space Systems," *Cybersecurity and Infrastructure Security Agency*, accessed September 3, 2026. (https://www.cisa.gov/topics/risk-management/space-systems); Cybersecurity and Infrastructure Security Agency, "Recommendations to Space System Operators for Improving Cybersecurity," June 2024. (https://www.cisa.gov/sites/default/files/2024-06/Recommendations%20to%20Space%20System%20Operators%20for%20Improving%20Cybersecurity%20%28508%29.pdf); Space Information Sharing and Analysis Center Chairman Samuel Visner, "Written Testimony," *Testimony before the U.S. House Committee on Homeland Security*, April 29, 2026. (https://docs.house.gov/meetings/HM/HM08/20260429/119218/HHRG-119-HM08-Wstate-VisnerS-20260429.pdf)

40. Sandra Erwin, "Space Information Sharing and Analysis Center to be based in Colorado Springs," *SpaceNews*, April 8, 2019. (https://spacenews.com/space-information-sharing-and-analysis-center-to-be-based-in-colorado-springs); Space Information Sharing and Analysis Center Chairman Samuel Visner, "Written Testimony," *Testimony before the U.S. House Committee on Homeland Security*, April 29, 2026. (https://docs.house.gov/meetings/HM/HM08/20260429/119218/HHRG-119-HM08-Wstate-VisnerS-20260429.pdf)

41. U.S. Government Accountability Office, "Space Supply Chains: Additional DOD Actions Could Strengthen Its Enterprise Approach for Managing Risks," November 17, 2026. (https://www.gao.gov/products/gao-27-108683)

42. Annie Fixler and Mariam Davlashelidze, "The Biden Administration Left Space Vulnerable to Cyberattack," *The Cipher Brief*, January 29, 2025. (https://www.thecipherbrief.com/column_article/the-biden-administration-left-space-vulnerable-to-cyberattack)

43. Space Information Sharing and Analysis Center Chairman Samuel Visner, "Written Testimony," *Testimony before the U.S. House Committee on Homeland Security*, April 29, 2026. (https://docs.house.gov/meetings/HM/HM08/20260429/119218/HHRG-119-HM08-Wstate-VisnerS-20260429.pdf)

44. "Securing Space: A Plan for U.S. Action," *Council on Foreign Relations*, accessed October 29, 2026, pages 28-29. (https://www.cfr.org/task-force-reports/securing-space/recommendations)

45. Space Infrastructure Act, H.R. 1154, 119th Congress, introduced February 10, 2025, section 2. (https://www.govinfo.gov/app/details/BILLS-119hr1154ih/related)

46. Satellite Cybersecurity Act of 2025, S. 3404, 119th Congress, as passed by the Senate September 23, 2026. (https://www.govinfo.gov/content/pkg/BILLS-119s3404es/xhtml/BILLS-119s3404es.html)

47. Anne Wainscott-Sargent, "It's Unanimous: Space Already Functions as Critical Infrastructure," *Via Satellite*, April 7, 2026. (https://www.satellitetoday.com/government-military/2026/04/07/its-unanimous-space-already-functions-as-critical-infrastructure)

48. Cybersecurity and Infrastructure Security Agency, "FY 2021 National Defense Authorization Act: Section 9002(b) Report," November 12, 2021, pages 44 and 49-50. (https://www.cisa.gov/sites/default/files/2023-01/Section_9002_NDAA_Report_FINAL_508c.pdf)

49. U.S. Department of Homeland Security, "FY 2021 National Defense Authorization Act Section 9002(b) Report," November 12, 2021, page 50. (https://www.cisa.gov/sites/default/files/2023-01/Section_9002_NDAA_Report_FINAL_508c.pdf)

50. The White House, "Letter from the President to Select Congressional Leadership on the Nation's Critical Infrastructure," November 7, 2022. (https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/11/07/letter-from-the-president-to-select-congressional-leadership-on-the-nations-critical-infrastructure); The White House, "National Security Memorandum on Critical Infrastructure Security and Resilience," April 30, 2024. (https://www.govinfo.gov/content/pkg/DCPD-202400358/pdf/DCPD-202400358.pdf)

51. U.S. Department of Commerce, Office of Space Commerce, "Cybersecurity Executive Order Includes Direction on Space Systems," January 17, 2025. (https://space.commerce.gov/cybersecurity-executive-order-includes-direction-on-space-systems)

52. Executive Office of the President, National Space Council and Office of the National Cyber Director, "Space System Cybersecurity: Space Industry Perspectives," January 2025, pages 2 and 6. (https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/Space-System-Cybersecurity-Industry-Perspectives-Report.pdf)

53. Ibid., pages 3-4. (https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/Space-System-Cybersecurity-Industry-Perspectives-Report.pdf)

54. Executive Order 14369, "Ensuring American Space Superiority," December 18, 2025. (https://www.whitehouse.gov/presidential-actions/2025/12/ensuring-american-space-superiority)

55. The White House, "National Security Science & Technology Strategy," August 2026. (https://www.whitehouse.gov/wp-content/uploads/2026/08/NSSTS-082026.pdf)

56. The White House, National Security Presidential Memorandum 17, "The National Space Transportation Policy," August 20, 2026. (https://www.whitehouse.gov/presidential-actions/2026/08/national-security-presidential-memorandum-nspm-17)

57. "Space Threat Fact Sheet," *U.S. Space Force*, accessed October 21, 2026. (https://www.spaceforce.mil/About-Us/Fact-Sheets/Fact-Sheet-Display/Article/4297159/space-threat-fact-sheet); Frank Cilluffo, RADM (Ret.) Mark Montgomery, Sharon Cardash, and Kelsey Shields, "Time to Designate Space Systems as Critical Infrastructure," *CSC 2.0*, April 2023. (https://cybersolarium.org/wp-content/uploads/2023/04/CSC2.0_Report_SpaceCriticalInfrastructureSector.pdf)

58. Commander of U.S. Space Command Gen. Stephen N. Whiting, "Fiscal Year 2027 Priorities and Posture of United States Space Command," *Testimony before the House Armed Services Committee, Subcommittee on Strategic Forces*, March 17, 2026. (https://www.spacecom.mil/Portals/57/2026%20CDRUSSPACECOM%20Posture%20Statement%20-%20Final.pdf)

59. U.S. Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2025," December 23, 2025, pages 21-22. (https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF)

60. Ibid., page 22. (https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF); U.S. Air Force, "Air Force Doctrine Publication 3-12: Cyberspace Operations," May 1, 2026, page 7. (https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-12/3-12-AFDP-CYBERSPACE-OPS.pdf)

61. U.S. Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2025," December 23, 2025, page 22. (https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF)

62. Audrey Decker, "China is practicing 'dogfighting' in space, Space Force says," *Defense One*, March 18, 2025. (https://www.defenseone.com/threats/2025/03/china-practicing-dogfighting-space-space-force-says/403863); Jack Burnham, "Showcasing Advanced Space Capabilities, China Displays 'Dogfighting' Maneuvers in Low Earth Orbit," *Foundation for Defense of Democracies*, March 21, 2025. (https://www.fdd.org/analysis/policy-briefs/showcasing-advanced-space-capabilities-china-displays-dogfighting-maneuvers-in-low-earth-orbit)

63. Commander of U.S. Space Command Gen. Stephen N. Whiting, "Fiscal Year 2027 Priorities and Posture of United States Space Command," *Statement before the Senate Armed Services Committee*, March 26, 2026, pages 5-6. (https://www.armed-services.senate.gov/imo/media/doc/whiting_opening_statement.pdf)

64. Andrew Jones, "China's Shijian-21 towed dead satellite to a high graveyard orbit," *SpaceNews*, January 27, 2022. (https://spacenews.com/chinas-shijian-21-spacecraft-docked-with-and-towed-a-dead-satellite)

65. U.S. Department of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2025," December 23, 2025, pages 21-22. (https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF)

66. Commander of U.S. Space Command Gen. Stephen N. Whiting, "Fiscal Year 2027 Priorities and Posture of United States Space Command," *Testimony before the House Armed Services Committee, Subcommittee on Strategic Forces*, March 17, 2026, pages 5-6. (https://www.spacecom.mil/Portals/57/2026%20CDRUSSPACECOM%20Posture%20Statement%20-%20Final.pdf)

67. Foreign, Commonwealth & Development Office , Press Release, "Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion," May 10, 2022. (https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion)

68. Viasat, Press Release, "KA-SAT Network cyber attack overview," March 30, 2022. (https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview)

69. Sandra Erwin, "Russia escalates rhetoric on commercial satellites, calls them 'legitimate targets for retaliation,'" *SpaceNews*, October 27, 2022. (https://spacenews.com/russia-escalates-rhetoric-on-commercial-satellites-calls-them-legitimate-targets-for-retaliation); Guy Faulconbridge, "Russia warns West: We can target your commercial satellites," *Reuters*, October 27, 2022. (https://www.reuters.com/world/russia-says-wests-commercial-satellites-could-be-targets-2022-10-27)

70. Max Hunder, "Russia tries to jam Musk's Starlink systems to counter Ukrainian drones," *Reuters*, July 8, 2026. (https://www.reuters.com/business/aerospace-defense/russia-tries-jam-musks-starlink-systems-counter-ukrainian-drones-2026-07-08)

71. Commander of U.S. Space Command Gen. Stephen N. Whiting, "Fiscal Year 2027 Priorities and Posture of United States Space Command," *Testimony before the House Armed Services Committee, Subcommittee on Strategic Forces*, March 17, 2026. (https://www.spacecom.mil/Portals/57/2026%20CDRUSSPACECOM%20Posture%20Statement%20-%20Final.pdf)

72. "Global Navigation Satellite System (GNSS) Outages and Alterations," *European Union Aviation Safety Agency*, accessed September 3, 2026. (https://www.easa.europa.eu/en/domains/air-operations/global-navigation-satellite-system-outages-and-alterations)

73. U.S. Space Command, Press Release, "Russian direct-ascent anti-satellite missile test creates significant, long-lasting space debris," November 15, 2021. (https://www.spacecom.mil/Newsroom/News/Article-Display/Article/2842957/russian-direct-ascent-anti-satellite-missile-test-creates-significant-long-last)

74. Ibid.

75. Commander of U.S. Space Command Gen. Stephen N. Whiting, "Fiscal Year 2027 Priorities and Posture of United States Space Command," *Testimony before the House Armed Services Committee, Subcommittee on Strategic Forces*, March 17, 2026. (https://www.spacecom.mil/Portals/57/2026%20CDRUSSPACECOM%20Posture%20Statement%20-%20Final.pdf)

76. Ibid.

77. National Intelligence Council, "Updated IC Gray Zone Lexicon: Key Terms and Definitions," July 2024, pages 4-5. (https://www.dni.gov/files/ODNI/documents/assessments/NIC-Unclassified-Updated-IC-Gray-Zone-Lexicon-July2024.pdf); U.S. Defense Intelligence Agency, "Challenges to Security in Space 2022," accessed October 29, 2026, page 44. (https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf)

78. North Atlantic Treaty Organization, "NATO's overarching Space Policy," June 27, 2019, paragraphs 2-4. (https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2019/06/27/natos-overarching-space-policy)

79. U.S. Space Force, "Future Operating Environment 2040," April 2026, pages 5-6. (https://www.spaceforce.mil/Portals/2/Documents/SAF_2026/Future_Operating_Environment_2040_Final.pdf)

80. Emmerson Overell, "Fly Me to the Moon: 4 Ways Artemis Builds on Apollo's Giant Leap," *Foundation for Defense of Democracies*, June 23, 2026. (https://www.fdd.org/analysis/2026/06/23/fly-me-to-the-moon-4-ways-artemis-builds-on-apollos-giant-leap); National Aeronautics and Space Administration, Office of Inspector General, "NASA's Management of the Human Landing System Contracts," March 10, 2026. (https://oig.nasa.gov/audits/nasas-management-of-the-human-landing-system-contracts)

81. "Commercial Crew Program," *National Aeronautics and Space Administration*, accessed September 3, 2026. (https://www.nasa.gov/humans-in-space/commercial-space/commercial-crew-program); "Commercial Lunar Payload Services," *National Aeronautics and Space Administration*, accessed September 3, 2026. (https://www.nasa.gov/commercial-lunar-payload-services); "Human Landing Systems," *National Aeronautics and Space Administration*, accessed September 3, 2026. (https://www.nasa.gov/reference/human-landing-systems-2);

82. Courtney Albon, "Space Command to Launch Wargame Series for Industry," *Air & Space Forces Magazine*, March 18, 2026. (https://www.airandspaceforces.com/space-command-to-launch-wargame-series-for-industry); Sandra Erwin, "U.S. Space Command to bring commercial firms into classified wargame on nuclear threats in space," *SpaceNews*, January 28, 2026. (https://spacenews.com/u-s-space-command-to-bring-commercial-firms-into-classified-wargame-on-nuclear-threats-in-space); Shannon Burns, "USSPACECOM hosts third wargame series focused on maneuver warfare in the space domain," *Defense Visual Information Distribution Service*, September 25, 2026. (https://www.dvidshub.net/news/575722/usspacecom-hosts-third-wargame-series-focused-maneuver-warfare-space-domain)

83. "Space Delta 10 - Wargaming, Field Experimentation, Doctrine & Lessons Learned," *U.S. Space Force Space Training and Readiness Command*, accessed September 3, 2026. (https://www.starcom.spaceforce.mil/About-Us/Units/Space-Delta-10-Doctrine-Wargaming)

84. The White House, "National Space Policy of the United States of America," December 9, 2020, page 19. (https://www.nasa.gov/wp-content/uploads/2023/10/nationalspacepolicy12-9-20.pdf)

85. U.S. Space Force, "Future Operating Environment 2040," April 2026. (https://www.spaceforce.mil/Portals/2/Documents/SAF_2026/Future_Operating_Environment_2040_Final.pdf)

About the Authors



Emmerson Overell is a project coordinator for FDD's Center on Cyber and Technology Innovation. She monitors threats to U.S. national security in the Arctic, space, and cyberspace domains. Emmerson holds an M.A. in security policy studies from The George Washington University and B.A.s in political science and Middle Eastern studies from the University of California, Santa Barbara.



Annie Fixler is the director of FDD's Center on Cyber and Technology Innovation and an FDD senior fellow. She works on issues related to cyber-enabled economic warfare, the national security implications of cyberattacks on economic targets, and U.S. cyber resilience.

The views of the authors do not necessarily reflect the views of CSC 2.0's distinguished advisors, senior advisors, or any affiliated organizations or individuals.

About CSC 2.0

CSC 2.0 is preserving the legacy and continuing the work of the Cyberspace Solarium Commission (CSC). Congress created the CSC in the John S. McCain National Defense Authorization Act for Fiscal Year 2019 to "develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequences." The commission operated successfully for two and a half years, publishing its flagship report in March 2020 along with subsequent white papers. The CSC issued more than 80 recommendations to reform U.S. government structures and organization, strengthen norms and non-military tools, promote national resilience, reshape the cyber ecosystem, operationalize public-private collaboration, and preserve and employ military instruments of national power.

At the CSC's planned sunset, the commissioners launched the CSC 2.0 project to support continued efforts to implement outstanding CSC recommendations, provide annual assessments of the implementation of CSC recommendations, and conduct research and analysis on several outstanding cybersecurity issues identified during the commission's tenure.

For more information, visit **www.CyberSolarium.org**.

Co-Chairmen

Angus S. King Jr., U.S. Senator for Maine

Mike J. Gallagher, Former U.S. Representative for Wisconsin's 8th District

Distinguished Advisors

Frank J. Cilluffo, Director of Auburn University's Charles D. McCrary Institute for Cyber and Critical Infrastructure Security

Tom Fanning, Former Chairman, President, and CEO of Southern Company

Chris Inglis, Former National Cyber Director

Jim Langevin, Former U.S. Representative for Rhode Island's 2nd District

Patrick J. Murphy, Former Acting Secretary and Under Secretary of the U.S. Army & Former U.S. Representative for Pennsylvania's 8th District

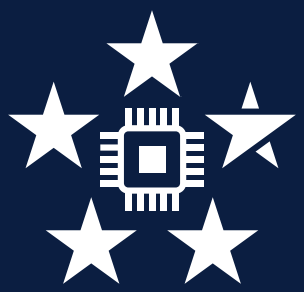
Samantha F. Ravich, Distinguished Fellow at the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies

Ben Sasse, Former U.S. Senator for Nebraska

Suzanne Spaulding, Senior Adviser for the Defense and Security Department at the Center for Strategic and International Studies

Partners

FDD | CCTI



CSC 2.0

Preserving and Continuing the Cyberspace Solarium Commission