CENSA Report:
Designating Critical Infrastructure in Space: A Matter of National Security in the AI Race

January 2026
Annslee Perego, CENSA Fellow

BACKGROUND

Artificial intelligence (AI) continues to permeate every aspect of our lives and is becoming more ingrained in our national security. To support AI's exponential growth, companies like Google are planning to launch data centers in space. Space-housed data centers could be a feasible solution to issues involving negative environmental consequences; however, this endeavor raises national security concerns since infrastructure in space is not afforded the same protections as critical infrastructure sectors in the United States (US). Infrastructure in space, including data centers, warrants special protections similar to critical infrastructure on earth, and US National Security will be at risk with space infrastructure until these regulatory protections are conceived.

TERRESTRIAL DATA CENTERS

Data centers are an important component of AI and national security. Data centers are the physical facilities that house the information technology and data storage components of AI. Tech giants like Microsoft and large investment companies like Blackrock are dedicating billions into constructing AI data centers in order to support AI's swift deployment, and the public sector places equal importance on the development of AI. The White House has repeatedly affirmed the importance of its development through Executive Orders and an AI Action Plan to set global standards, capitalize on military and economic benefits, and remain a global leader over competitors such as China. While the growth opportunities of AI are vast, the negative aspects of data centers may hinder their construction on Earth, stunting the research and development of AI technology.

Environmental concerns plague the expansion of terrestrial data centers due to the sheer amount of water and energy used by the infrastructure. Data centers are rooms made up of servers, and the heat must be removed from the room to avoid overheating. This is typically accomplished through water-intensive cooling towers and water evaporation-assisted air cooling. A large data center can require up to 5 million gallons per day just to cool the hardware, and replying "thank you" alone to ChatGPT can use "40 to 50 milliliters of water to generate a three-word 'You are welcome' response from ChatGPT."

Data centers also require copious amounts of energy to operate, which depending on the source of energy, also requires water. They necessitate an interminable power supply, and some estimate that the amount of energy needed to power this 24/7 technology in the US alone could consume more than the entire country of Japan by 2030. Stated another way, by 2026, Data centers are expected to consume 1,050 terawatt-hours of energy, which could cause significant strain on the energy grid. By comparison, 10,500 kilowatthours are needed to power the average US home for one year, or approximately 0.000001% of the energy needed to power data centers. This new

demand for energy places significant strain on the power grid as energy companies struggle to create feasible solutions to AI's unquenchable need for energy. The profuse amount of water in tandem with the amount of energy needed for this technology creates nontrivial environmental burdens.

EXTRATERRESTRIAL DATA CENTERS

Data centers in space would create an almost dream-like solution to almost all of its earthly environmental concerns. The need for liquid server cooling would be eliminated, because servers would not need to be housed within the four walls of a building like they are on earth. Extraterrestrial data centers can take advantage of the openness of space and "use the vacuum of deep space as an infinite heat sink" by "emitting waste heat from infrared radiation into space." Solar energy would be abundantly available, creating a constant source of clean energy and eliminating the need for other energy sources and relieving pressure on electric grids. Superfluous access to high-intensity solar power has the potential to drastically lower energy costs and produce less carbon emissions as an abundant clean energy source. Physical space is virtually unlimited, further creating a ripe opportunity for launching data centers in space.

The concept of space data centers has its own hurdles, such as the expense associated with launches and latency issues. However, that hasn't stifled big tech's desire to launch data centers in space. Companies like Nvidia already tout that, "[e]xtraterrestrial data centers are just on the horizon," and startups like Starcloud are already developing orbital data centers to support AI development with initial launches scheduled in 2026. Axiom Space has announced the launch of its first two orbital data center nodes by the end of 2026, and claims to provide "secure, scalable, and cloud-enabled data storage and processing" and AI solutions. With many projects underway for space data centers in the near future, it is imperative these infrastructures are adequately protected.

NATIONAL SECURITY CONCERNS

Extraterrestrial data centers will create exciting opportunities for AI's further development, but housing AI infrastructure in space is a national security concern due to lack of regulatory protections under US law. Satellites are already subject to cyberattacks and espionage, and data centers incumbent to develop AI will attract these same types of attacks. In 2023, the National Counterintelligence and Security Center issued a warning to the space industry that foreign intelligence agencies are using cyberattacks and other means of gaining access to the US Space industry in order to steal intellectual property, disrupt US satellites, and cause economic harm to the US commercial space sector. Data centers in space would be foreign intelligence agencies' next target. The US should prioritize protecting these assets to ensure national security and the future of AI in a similar manner to critical infrastructure sectors.

To protect terrestrial infrastructure from these types of threats, the US defines 16 sectors as critical infrastructure, but space infrastructure is not presently included. Critical infrastructure

sectors[1] are defined as"systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." This designation allows the federal government to prioritize the protection of the sectors and allocate key resources to identify vulnerabilities, develop protection measures through industry partnerships, and provide means of rapid recovery during emergencies. Space infrastructure is not designated amongst any of these sectors, despite the fact that space infrastructure already plays a significant role in everyday life. The US relies on satellites to provide a variety of critical needs, such as the Global Positioning Services (GPS) that enable everyday services related to navigation and timing; phone and internet providers use services through fixed satellites to enable worldwide communications; and meteorological satellites that have revolutionized weather forecasting. The US reliance on space infrastructure is ever-growing, especially with the prediction of launching extraterrestrial data centers.

Despite increasing reliance on space infrastructure, multiple failed legislative attempts have demonstrated that the current critical infrastructure designation is not easily malleable to space. The proposed Space Infrastructure Act of 2023 would have directed DHS to designate space systems, services, and technology as the 17th critical infrastructure sector. However, the bill died in the House Committee on Science, Space, and Technology. The Space Infrastructure Act of 2025 contains largely the same text and goal of the Space Infrastructure Act of 2023, but it has gained little traction. The bills both recognize that the space industry needs some type of federal protection or regulation but have been unable to provide any statutory protections to space infrastructure. The bills were likely unsuccessful due to their broad scope, which essentially designates the entirety of space as critical infrastructure.

The crux of failure is that these proposed bills only apply the concept of critical infrastructure as we understand it on Earth instead of considering the unique needs of space. In order to protect critical space infrastructure, legislators should begin thinking about what aspects of space activities are critical instead of attempting to fit space within the current model of critical infrastructure. This mindset shift will help the US to develop a regulatory regime that is specific to space and the critical functions housed within its open plains, rather than attempting to fit it within a terrestrial definition of critical infrastructure.

POLICY RECOMMENDATIONS

A comprehensive legislative solution could take years to develop. Since vital infrastructure like GPS and telecommunications is already housed in space, we need to consider short-term and long-term solutions for protecting space assets:

[1] Among the 16 sectors are the chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government services and facilities, healthcare and public health, information technology, nuclear reactors, materials, and waste, transportation, and water and wastewater.

1. DHS, who is tasked with coordinating and implementing the National Security Memorandum on Critical Infrastructure and Security Resilience, should consider current critical infrastructure sectors as inclusive of space infrastructure that may affect them. For example, the communications critical infrastructure sector should include satellites that are an essential part of telecommunications or the information technology sector should include data centers when they are eventually launched. This is a short-term solution until specific space critical infrastructure regulation is developed, because there will be space infrastructure that is not directly tied to an earth-bound sector. This is a temporary measure to protect systems and structures with a direct impact on Earth.

2. Private/public partnerships, which will likely carry out the majority of space endeavors, should create comprehensive incident response plans to protect space assets. These partnerships will be a pillar of space infrastructure, similar to critical infrastructure on Earth;[2] thus, companies should create partnerships with other companies, domestic and foreign government organizations, and academic partners who will be able to assist if an incident occurs. Companies should also prioritize implementing an incident response plan prior to any space endeavor to prevent incidents and be prepared if one occurs. Protecting private assets will be essential to the security of space infrastructure.

3. Congress should create a new model for critical infrastructure in space. Instead of trying to fit space infrastructure into the definitions of critical infrastructure on earth, Congress should conceive a new directive that protects space assets separate from the earth critical infrastructure sectors. This new model should prioritize protection of space infrastructure that has a direct tie to domestic critical infrastructure sectors as well as assets that will have vital importance to the success of space missions that may not have a direct correlation on Earth. This ultimate solution will help create tailored protections for infrastructure in space that aren't limited to earth-bound definitions.

This report is the product of a policy working group sponsored by the Council for Emerging National Security Affairs. The views and policy recommendations are the authors' own and do not reflect an official position of CENSA or its board members.

[2] In the energy sector alone, eighty percent of the critical infrastructure is privately owned. Private companies already play a significant role in terrestrial infrastructure, and the same will be true of space infrastructure.