SPACE FOUNDATION

THE SPACE REPORT

THE AUTHORITATIVE GUIDE TO GLOBAL SPACE ACTIVITY

2021 Q2

2020 GLOBAL SPACE ECONOMY | PRESIDENT BIDEN'S SPACE BUDGET | MIDYEAR LAUNCH UPDATE




Space Is Critical Infrastructure; Securing It Is a National Imperative

Edward Swallow and Samuel Visner are founding members of the Space Information Sharing and Analysis Center (Space ISAC). They are calling on Congress to support a recent proposal to include space assets as crucial to national security and economic well-being.

Edward Swallow is senior vice president of Civil Systems Group. Prior to CSG, he was vice president, Business Development for the Federal and Defense Technologies Division, Northrop Grumman Information Systems.

Samuel Sanders Visner is a Technical Fellow at the MITRE Corporation and serves as member of the Cyber Council of the Intelligence and National Security Alliance and the Cyber Committee of the Armed Forces Communications and Electronics Association.

The U.S. space enterprise is in the midst of a transformative policy era that will significantly shape the future of our society, the robustness of our economy, and America's role within the global community. The public and private sectors are collaborating to conceptualize and invest in the development of a vibrant, near-future space economy and the engineering, manufacturing, and infrastructural commitments that will underpin it.

To ensure this economy achieves its full potential, we must commit and act to preserve its foundations amid a dynamic threat environment. We've recently witnessed at great cost how supply chain disruptions[1] and cyberattacks on critical infrastructure like fuel pipelines[2] can wreak havoc on the lifeblood of domestic communities and global trade alike. Such an attack on key technology in the space domain could have similarly devastating effects.[1]

As leaders in the White House and Congress discuss how to shore up our nation's terrestrial infrastructure, they are also turning their eyes skyward to consider a specific, crucial, and feasible policy action for securing space. A bipartisan bill recently introduced in Congress would designate space systems as critical infrastructure in the national interest — a concept that has wide support within the space enterprise. Doing so is an imperative to ensure the resiliency of space assets and foster the continued development of our society and economy, both on Earth and in space.

Why We Must Bolster Space Resiliency

In the United States — and arguably all industrialized nations — our lifestyle, economy, and national security depend upon thousands of space systems in orbit. For instance, the Global Positioning System (GPS) makes daily activities for individual citizens easier and enables global shipping and transportation, including ground, air traffic, and marine navigation. Much of the activity enabling modern communications networks and information processing leverages space-based infrastructure, which will be connected, in turn, to global cloud networks. The U.S. Armed Forces have also long relied upon satellite capabilities for command and control, missile guidance, early warning, and intelligence capabilities.

This discussion is not about space as a place; otherwise, the argument could be made for oceans and airspace likewise being critical sectors. This is, rather, a discussion about space systems — and the data they gather, distribute, and process — as integral elements of almost every other sector, each of which does not necessarily have the expertise or interest to engage on issues unique to space.

The degree to which space systems impact our society is the result of a rapidly evolving space ecosystem, both in terms of the dramatically decreasing cost of access to low Earth orbit and the swiftly increasing capability of small satellites to do big things. Just two decades ago, space operations were limited to large, specialized, and expensive systems. These systems were managed by a small group of space operators and featured their own dedicated networks. Today, there are more than 4,000




active satellites — and far more in prospect — operating in a complex, emerging space ecosystem that comprises assets of the U.S. government, commercial, and even foreign-government and foreign-owned nongovernmental space operators and systems.

According to the Bank of America, the space industry could triple to $1.4 trillion by 2030.[3] By then an estimated 50,000 satellites could be in orbit, many connected to public communication networks. With the commercial space sector maturing rapidly and introducing ever more potential targets into a cyber-contested domain, it's vital that we bolster space system resiliency now to enable our present economy's viability and to foster continuing growth and innovation into the future.

Counterspace Risks, Threats and Vulnerabilities

Space systems are increasingly vulnerable to cyber disruption. Going as far back as 1998, a U.S.-German ROSAT X-Ray satellite reportedly was compromised,[4] causing its power systems to fail. Media reports indicate that China was a potential culprit[5] in a more recent incident that compromised the command and control of NASA satellites, and other efforts to compromise space systems have been observed.

That threat is front and center today. As Lt. Gen. Stephen Whiting, commander of Space Operations Command, said last year[6] while serving as U.S. Space Force deputy commander: "We know that cyberattack is where we are most likely to face the enemy in space." Inadequate cybersecurity requirements and governance have led to a variety of major cybersecurity vulnerabilities throughout space system infrastructure, including insider threats, supply chain vulnerabilities, communications cryptography, cyber best practices for ground systems, and diminished situational awareness.

Previous attempts to protect space systems assumed that safeguarding ground segments meant protecting the whole system. However, modern attack vectors are much more diverse and dispersed, with global exposure to user, on-orbit, and link segments. Ground systems, which are connected to public information networks, are built from commoditized parts and technologies that lack uniform cyber resiliency. Modern satellites — while subject to equal physical, power, and cost constraints — are likewise built from disparate parts with varying cyber protections. We must ensure cybersecurity is built into all of these systems.

Satellites are also beholden to orbital mechanics and cannot simply be told to avoid threats. They must be active to do their jobs. As a result, bad actors can always see and reach out to the central nodes of the system. There is no uniform approach to "zero trust" for space systems that is now a standard of modern IT systems. If a threat breaches the communications link between physical ground and space segments or compromises any component within a segment, then the entire system is compromised. Open-source and commercial solutions available today are insufficient to fully inoculate space systems from cyber threats, and legacy space systems are particularly at risk.

While the Communications Critical Infrastructure sector protects communications satellites, who is coordinating policy, strategies, programs, and resources to protect the systems that launch and operate them, along with GPS and other satellites? What about the companies that manufacture, launch, or operate space vehicles or the supply chains that sustain all these space systems?

No government entity currently coordinates this important national responsibility. It is vital to designate this responsibility to help foster consensus on standards and best practices among spacefaring governments and commercial entities. Ignoring these vulnerabilities now, especially given long development and acquisition cycles, could lead to graver, longer-term security risks to the entire space domain. A critical infrastructure designation would help immediately alleviate these vulnerabilities.




What a Critical Infrastructure Designation Means for Space

Taking the deliberate policy action to designate space systems as critical infrastructure would accomplish much toward securing space and ensuring a robust space economy:

- Most directly, a critical infrastructure designation would add protections to manufacturing and supply chains for other satellites, space vehicles, and components while extending the protections already in place for communications satellites to their launch and mission systems.
- The U.S. would make clear that space systems security and resilience are national priorities through such a declaration, which would send a signal to those who would harm our systems of our serious intent to defend our national and economic security in space.
- A critical infrastructure designation would catalyze policymakers and a national stakeholder community comprising government and private sector entities focused on space systems security and resilience to coordinate efforts to protect the space industry on which we all depend.
- It would enable the industry to consolidate and amplify efforts to build collaboration among manufacturers, suppliers, owners, and operators while driving global consensus regarding best practices and information sharing, building on the work of the Space Information Sharing and Analysis Center (Space ISAC) and its Threat Intelligence Watch Center.
- Collaboration would drive consensus on prioritizing defense-in-depth[7] (DiD) risk management postures to harden space systems. All systems, hardware, firmware, and software — whether developed through traditional or agile engineering— should feature cyber-hardened designs with risk-based DiD cyber protections applied across all segments to detect, deter, and attribute attacks and overcome the risk of adversaries breaching systems and operating unhindered inside them.
- Space system owners and operators would also be empowered to adopt baseline, threat-informed, risk-based engineering and design cybersecurity postures because they would have better ability to document and identify threats. With such knowledge, owners and operators can adopt appropriate risk tolerances and tailored controls and requirements for mission duration, spacecraft size, and maneuverability in space while minimizing undue burden.

Promising Policy Developments

There is momentum abroad and here at home to prioritize the security of space infrastructure. Last year,[8] the European Commission — the European Union's (EU) executive body — authored legislation to revise governance of Union-wide cybersecurity standards for critical economic and societal sectors; space systems have been added to the EU's list of critical sectors.

Just this month, U.S. Reps. Ted Lieu (D-California) and Ken Calvert (R-California) introduced bipartisan legislation to establish space as a 17th sector of critical infrastructure as classified by the Department of Homeland Security (DHS). "Space is infrastructure," Rep. Lieu argued in a joint press release,[9] noting the pivotal role space plays in daily life. "As a result, we have to ensure that we're protecting these critical systems by directing the right minds and resources towards them."

The Space Infrastructure Act as introduced in the House of Representatives ensures that U.S. assets in space — including orbiting satellites, space vehicles, launch systems and infrastructure, manufacturing facilities, supply chains, and associated communications and information technology — receive thorough security scrutiny and analysis.

If passed, the bill would direct DHS to partner with other federal agencies and departments and the Space ISAC to issue guidance about space infrastructure's scope. This guidance would designate the U.S. government's leadership team on this issue, including a Sector Risk Management Agency to oversee space infrastructure and appropriate entities to support this oversight.

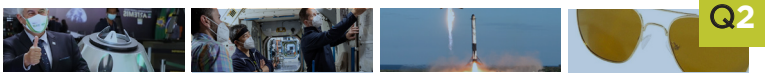



"The collaboration between federal security agencies and industry partners directly and indirectly involved with space-based assets and technologies is essential to America's future as we confront evolving threats," Calvert said in the same press release.

In our capacities as founding members of the Space ISAC — which has formally endorsed this legislation — we applaud this development and stand ready to provide guidance, expertise, and analysis to the U.S. government as it moves to secure space.

Our dependence on space is greater than ever before, and it will continue to deepen at a near-exponential rate. Access to space is not just vital to the national and economic security of the U.S. and our allies: It is also vital to China, Russia, North Korea, and other potential adversaries.

Inaction on securing space cedes a strategic advantage to these adversaries. We must act in a deliberate, meaningful way to outpace these threats. By designating the space systems as critical national infrastructure, the U.S. can secure these pivotal capabilities to assume and maintain a stronger space position within the international community, today and in the future.



SPACE FOUNDATION

Thomas Dorame
Sr. Vice President

RESEARCH & ANALYSIS

Lesley Conn
Senior Manager

Becki Yukman
Senior Data Analyst

Matt Christine
Data Analyst

CONTRIBUTORS

SPACE INVESTMENT SERVICES

Micah Walter-Range
Director of Research
Space Investment Services LLC

Dr. Mariel Borowitz
Assistant Professor
Sam Nunn School of
International Affairs,
Georgia Institute of Technology

Courtney Stadd
Tara Larson
Contributing Writers

Patrick Harper
Ryan Russell
Researchers

Steve Edelman
Editor

Shawn Huff
Wendy Perelstein
Web Support

Design Development Team
ROMIE LUCAS
graphic design & illustration

QUILTY analytics

Chris Quilty
Founder and Partner
Quilty Analytics

Justin Cadman
Partner
Quilty Analytics

SPACE ISAC

Edward Swallow
Samuel Sanders Visner




Space Is Critical Infrastructure; Securing It Is a National Imperative

1 "The Ship That Blocked the Suez Canal May Be Free, But Experts Warn the Supply Chain Impact Could Last Months." CNBC.com. March 29, 2021. https://www.cnbc.com/2021/03/29/suez-canal-is-moving-but-the-supply-chain-impact-could-last-months.html. Accessed June 1, 2021.

2 "Cyberattack Forces a Shutdown of a Top U.S. Pipeline." The New York Times. May 13, 2021. https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html. Accessed June 1, 2021.

3 "Bank of America expects the space industry to triple to a $1.4 trillion market within a decade." CNBC.com. Oct. 4, 2020. https://www.cnbc.com/2020/10/02/why-the-space-industry-may-triple-to-1point4-trillion-by-2030.html.. Accessed June 1, 2021.

4 ROSAT. NASA Space Science Data Coordinated Archive. https://nssdc.gsfc.nasa.gov/nmc/spacecraft/display.action?id=1990-049A. Accessed June 14, 2021.

5 "China Key Suspect in U.S. Satellite Hacks: Commission." Reuters. Oct. 28, 2011. https://www.reuters.com/article/us-china-usa-satellite/china-key-suspect-in-u-s-satellite-hacks-commission-idUSTRE79R4O320111028. Accessed June 1, 2021.

6 "Cyber Attack Most Likely Space Threat: Maj. Gen. Whiting." Breakingdefense.com. Sept. 16, 2020. https://breakingdefense.com/2020/09/cyber-attack-most-likely-space-threat-maj-gen-whiting. Accessed June 2, 2021.

7 "Defending Spacecraft in the Cyber Domain." Center for Space Policy and Strategy. November 2019. https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf. Accessed June 1, 2021.

8 "Proposal for Directive on Measures for High Common Level of Cybersecurity Across the Union." European Commission. Dec. 16, 2020. https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union/ Accessed June 1, 2021.

9 "Reps. Lieu and Calvert Introduce Bill to Designate Space as Critical Infrastructure." Lieu.house.gov. June 4, 2021. https://lieu.house.gov/media-center/press-releases/reps-lieu-and-calvert-introduce-bill-designate-space-critical. Accessed June 14, 2021.




SPACE FOUNDATION

SPACE FOUNDATION'S MISSION:
Be the preeminent resource for space education, a trusted source of space information, and a provider of exceptional forums for the exchange of ideas.

As a 501(c)(3) nonprofit organization, philanthropic support is vital in fueling the Space Foundation's important programs and services. Every gift is significant in funding our work to **inspire**, **educate**, **connect**, and **advocate** for the global space community.

Discover the impact of giving at www.SpaceFoundation.org/Donate

SPACE FOUNDATION HQ

4425 Arrowswest Drive
Colorado Springs, CO 80907
+1.719.576.8000

WASHINGTON, D.C.

1700 North Moore Street, Suite 1105
Arlington, VA 22209

www.SpaceFoundation.org