SPACE ISAC

Developing a Sustainable Space Domain

The Space ISAC’s response to the United States National Space Council Space Priorities Framework

ABSTRACT

The Space Information Sharing and Analysis Center (Space ISAC) advocates for the responsible use of space and associated space-related activities. In alignment with the United States Space Priorities Framework, December 2021, the Space ISAC will focus on and advocate in the near-term for work-force development and the continued emphasis on science, technology, engineering, and mathematics (STEM) education to support space activities; the enhanced use of space in support of climate change; and the establishment of norms, which should include a discussion leading to the end of destructive anti-satellite (ASAT) testing in outer space. The Space ISAC also supports responsible behavior in space for all actors, and as such, developed three key pillars around developing norms and behavior for collective security, adopting space evolutions, and ensuring access to universal public-private sharing of threats. At such a key inflection point where space infrastructure is nearly indivisible from a functioning society, it is imperative to ensure the preservation of the space domain.

INTRODUCTION

"Space activities are essential to our way of life".

United States Space Priorities Framework, December 2021 [1]

Space has truly become an indispensable part of daily life. From navigation, timing, weather, communications, mapping, remote sensing, and support to all our country's National Critical Functions, space enables and provides humankind with economic opportunities and is vital to our national and economic security. The Space Information Sharing and Analysis Center[α] (Space ISAC) advocates for the responsible use of space and associated space-related activities. Irresponsible or ill-natured behavior in space will have negative impacts on economic and strategic security on a global scale.

The Space ISAC was established in Colorado Springs in 2019 and began formal operations in February 2021. As a member of the National Council of ISACs (NCI), it collaborates and coordinates with other Sector-based Information Sharing and Analysis Centers (ISACs). The NCI is a true cross-sector partnership, providing a forum for sharing threats, both cyber and physical, and mitigation strategies among other ISACs, government partners, and private sector partners during steady-state conditions and incidents requiring cross-sector response.

The Space ISAC established a mission statement to encompass collaboration across the global space enterprise:

> "The Space ISAC serves to facilitate collaboration across the global space industry to enhance our ability to prepare for and respond to vulnerabilities, incidents, and threats; to disseminate timely and actionable information among member entities; and to serve as the primary communications channel for the sector with respect to this information" [2].

This collaboration is vital to ensure the protection of our critical space assets, which impact many aspects of everyday life.

The Space ISAC strongly supports the United States Space Priorities Framework as published by the National Space Council. The activities described in the Framework align with the goals that established the Space ISAC. The following activities in which the Space ISAC will focus and

[α] https://s-isac.org/

for which it will advocate in the near-term are noteworthy: workforce development and the continued emphasis on science, technology, engineering, and mathematics (STEM) education to support space activities; the enhanced use of space in support of climate change; and the establishment of norms for responsible behavior in space, which should include a discussion leading to an end to destructive anti-satellite (ASAT) testing in outer space. Additionally, the Space ISAC will continue to develop and socialize our Pillars and Guiding Principles for all actors in the space domain.

The Space ISAC supports the continued emphasis on workforce development and the focus on the science, technology, engineering, and mathematics (STEM) education to support space activities. Access to and exploration of space will be enabled by this focus to innovate and open the universe to possibilities that will inevitably support our national security and economic development.

Space has a critical role in the monitoring of the environment with earth observation satellites. The Space ISAC supports and advocates for the collaboration of the federal government with the private sector to monitor and better understand the impacts of climate change across the world. Climate change is now recognized by the defense and homeland security communities, as well as key economists, as a threat to national and economic security. Space systems provide remote sensing data vital to understanding and building strategies requisite to confronting this threat.

The Space ISAC supports the establishment of norms of responsible behavior in space for all space actors; this includes development of cyberspace norms as well. The recent United Nations'[β] action establishing an Open-Ended Working Group (OEWG) to reduce "space threats through norms, rules and principles of responsible behavior" [3] and the "Tenets of Responsible Behavior in Space" memo [4] signed by Secretary of Defense Lloyd Austin III are promising. Further, the Space ISAC supports a ban on destructive, debris-generating anti-satellite (ASAT) testing in space. Irresponsible actions creating long-lived debris in space threaten the safety and security of the space domain.

The Space ISAC developed three key pillars around developing norms and behavior for collective security, adopting space evolutions, and ensuring access to universal public-private sharing of threats; and associated guiding principles to address the needs of the global space community, which includes commercial, government, and international space organizations. They strive to create innovative public-private partnerships, evolve guidance on resilience, and integrate space communities of interest. The Space ISAC is dedicated to cultivating a unique and innovative public-private partnership framework for the advancement of secure space solutions.

We are at a key inflection point where we must ensure the preservation of the space domain – there are economic, climate, and national security issues at risk. The Space ISAC finds itself in a unique opportunity to broaden the sharing of threat information with global space actors through collaboration to protect space assets and ensure the continued use of the space domain. Space is vital to all aspects of society; we must continue to engage the international community to preserve its use for future generations.

[β] https://www.un.org/en/

STEM WORKFORCE DEVELOPMENT NEEDS

As emphasized in the United States Space Priorities Framework, the continued strategic development of a wide range of STEM focus areas is imperative to meet the needs of current space activities, as well as the rapidly accelerating near-future space economy. Education and talent pipelines must be advanced and broadened to support the burgeoning new space age, especially since many of the needed knowledge areas are already extremely highly sought-after fields in the terrestrial realm. The following list encompasses some, though not all necessarily, of the critical fields necessary to support current and future space activities:

Cybersecurity (across all segments including Space, Ground, User, and Communication Links)

- Computer Science (AI, embedded systems, etc.)
- Engineering (Mechanical, Thermal, Chemical, Aeronautical, Electro Optical, Electronic, Electrical, Systems, etc.)
- Spectrum Communications (wired, RF, optical, etc.)
- Mathematics
- Physics (Space-related, such as orbital mechanics, radiation, etc.)

The ubiquity of these essential fields in terrestrial roles and applications leads to short supply and high competition for adequately trained and skilled members of the workforce.

The Space ISAC and the space systems industry recognize the challenges associated with building out a robust workforce that is prepared to fill the needs presented by the escalating space economy and the space activities in support of that domain. According to a Pew Research Center[χ] analysis of U.S. government data [5], these workforce obstacles are intensified by the unequal access and representation of different demographics into STEM fields. The Pew research states that "even with dramatic growth in the number of STEM graduates from U.S. colleges and universities at all degree levels since 2010, there is little indication that diversity in related jobs will shift substantially in the near term". To compete in the new global space economy, underrepresented workforce pools must be empowered, developed, and introduced to the space domain.

In addition to underrepresented workforce pools, another challenge that adds complexity to the issue of developing the space STEM workforce is that knowledge and awareness of the space domain is required in addition to the base STEM skills. While the critical skills previously listed are extremely competitive in their own rights, additional knowledge must be developed on top of those foundational domains to effectively translate those skills into the space domain.

For example, the physical environmental hardships of space greatly influence all aspects of engineering. Current space vehicle resource limitations on processing power and communications bound the capability available for critical functions such as cybersecurity and software that is developed to run on space vehicles. Understanding these types of limitations is critical for the education and development pipeline as the pipeline matures towards producing a space domain-ready workforce.

The Space ISAC also recommends ensuring that part of the STEM development pipeline is the socialization and communication of space vulnerabilities, incidents, and threats throughout the STEM workforce development pool to ensure that resilient, secure space solutions are being developed across all space-related STEM domains. This aligns with the Space ISAC guiding principle of encouraging integrated space communities of interest and ideation, which are considered key

[χ] https://www.pewresearch.org/

elements to foster global alignment to keep pace with the evolving space threat landscape.

Timing and methodology for introducing STEM into education is also important. Cybersecurity engineers often say that security should be "baked in" rather than "bolted on" after a system has been developed. This is necessary to gain benefits from secure designs which are more costly to change later in development. The same is true with STEM education.

Educators agree that incorporating STEM education into early education is "critical and developmentally appropriate" [6] to improve STEM literacy. Furthermore, increasing familiarization with unique challenges and opportunities of the space domain at an early age enables earlier educational-pathway decisions and consideration of space-sector careers. The Space ISAC recognizes this advantage and encourages early STEM education and outreach programs designed to increase awareness of space-related professions.

The National Science Board[δ] states that "assessing, enabling, and strengthening workforce pathways is essential to the mutually reinforcing goals of individual and national prosperity and competitiveness" [7]. The Space ISAC posits that this is even more true in the space domain, where investment into development of a diverse, equitable, accessible, and inclusive generation of skilled workforce with the unique additional layer of an understanding and knowledge of operating in space is a critical component for the ability of the United States to remain competitive as leaders in space.

SPACE AND CLIMATE CHANGE

The Biden Administration's Interim National Security Strategic Guidance identified climate change as one of "the biggest threats we face", it knows "no border or walls, and must be met with collective action" [8]. The administration followed up in October 2021 and the White House released a Fact Sheet [9] and its Report on the Impact of Climate Change on Migration [10] which again prioritized climate change as central to our national security. Additionally, the Department of Defense[ε] [11], the Intelligence Community [12], and the Department of Homeland Security[ϕ] [13] have expressed concerns regarding climate change and its implications to our national security and the security of our allies and partners.

The United States Space Priorities Framework specifically calls out space capabilities to not only address the ability to protect people, property, and the environment from extreme weather events, but to also address the climate crisis. It states that "the United States will advance the development and the use of space-based earth observation capabilities to support action on climate change" [1].

Earth observation satellites can and have played a crucial role in monitoring the causes, results, and impacts of climate change. Satellites offer a global view of the Earth's surface and atmosphere, which can provide invaluable data for monitoring glaciers, sea levels, agriculture, river levels, flooding, and numerous other earth-based activities related to the environment and the climate.

The recent United Nations Office for Outer Space Affairs[γ] (UNOOSA)/Austria World Space Forum focused on topics of "Space 4 Climate Action" [14]. The presenters provided examples of space capabilities addressing issues of climate change and public-private partnerships and collaborations to address these climate issues.

Satellites have been available and used to study the impacts to the environment since the launch of

[δ] https://www.nsf.gov/nsb/

[ε] https://www.defense.gov/

[ϕ] https://www.dhs.gov/

[γ] https://www.unoosa.org/

National Aeronautics and Space Administration's[η] (NASA) Landsat in 1972 [15]. Landsat 9 – a joint mission between the Department of the Interior's US Geological Survey[ι] (USGS) and NASA – was launched on September 27, 2021. According to the USGS, one of Landsat's missions is to "understand the impacts of climate change" [16]. The data from Landsat 9 will continue to be made available for free to the public as has been the case since 2008. Free and open data provide opportunities for continuous monitoring of Earth to identify fluctuations due to changes in climate.

The European Space Agency[φ] (ESA) and NASA have partnered with SAP to provide data from earth observation satellites to businesses to understand their impact on the environment [17]. The opportunities for the exploitation and use of earth observation data are growing.

The United States – in collaboration with our allies, partners, and the commercial remote sensing sector – collectively possess incredible resources and have tremendous opportunity to use space assets to monitor and respond to climate changes. The challenge, though, is in developing a comprehensive, integrated picture of the environment and implementing accessibility for public use. Accessible data will lead to more comprehensive research.

As the international community shares meteorological [18] and space environmental [19] information, opportunities exist for governments to collaborate with each other and commercial earth observation companies to integrate and provide earth observations for the study of the impacts related to climate change.

The technology is available and becoming more capable with larger constellations and smaller satellites. Companies like Maxar[κ] and Planet[λ] provide exceptional capabilities for the continuous monitoring of the environment. Integrating data from myriad sources enables the production of a holistic view to provide the data necessary to support the focus on climate change.

Earth observation satellites provide a superior capability to monitor impacts related to climate change. With a focus on climate change, we must use all available resources to aid in solving the climate issues. This includes ensuring that policies support the strategies for the more effective use of earth observation assets. Historically, satellite data has been restricted [20] due to economic or national security policies. These policies must align with technology to unleash the collective power of the public-private partnerships to help monitor and solve our climate crisis.

RULES AND NORMS FOR SPACE

The United States Space Priorities Framework makes clear that "The United States will defend its national security interests from the growing scope and scale of space and counterspace threats" [1]. The security and resilience of space systems are vital to our national and economic security, business and critical infrastructures, ability to marshal our military forces, and capacity to support our global commitments.

Threats to the space systems on which we and other critical infrastructures depend include those that can be targeted against specific space systems, as well as those that undermine the ability of the United States, our allies and partners, and the international system generally to make effective use of the space domain. The former consists of cyber and kinetic threats against space systems, including assets on-orbit, ground systems, the

[η] https://www.nasa.gov/

[ι] https://www.usgs.gov/

[φ] https://www.esa.int/

[κ] https://www.maxar.com/

[λ] https://www.planet.com/

workloads space systems support, and the manufacturing and support infrastructures on which space systems rely. The latter is comprised largely of irresponsible acts, such as a recent anti-satellite (ASAT) test conducted by Russia, leaving in orbit over 1,500 pieces of debris – some of which may pose risk to space systems, including the International Space Station.

The Space ISAC and the space systems industry, in collaboration with the United States Government, is continuing to develop information sharing and other operational capabilities requisite to strengthening the security and resilience of space systems. However, these efforts should be accompanied by efforts to create and strengthen norms observed by all space domain participants. These norms should be designed to eliminate acts dangerous to the operation and support of specific space systems, as well as to eliminate acts that place at risk the ability to use the space domain safely, such as ASAT tests conducted irresponsibly.

At the same time, the Government of the United States is building a national strategy for the protection of our space systems, aspects of which are described in the Framework. The Government is also addressing the need to strengthen the cybersecurity and resilience of our national security, and our economic, business, and critical infrastructures via those recommendations of the Congressional Solarium Commission enacted into law in the 2021 National Defense Authorization Act [21]. These provisions signal the increasing resolve of the United States to defend its national security and economic interests in cyberspace. In a global context, the United States has joined the "Paris Call for Trust and Security in Cyberspace," making clear our country's commitment to "open, secure, stable, accessible, and peaceful cyberspace" [22]. In joining the Call, the U.S. notes:

"Our decision to support the Paris Call reflects the Administration's pledge to renew America's engagement with the international community, including on cyber issues. We are committed to working alongside our allies and partners to *uphold established global norms in cyberspace and ensure accountability for states that engage in destructive, disruptive, or destabilizing cyber activity"* [22].

Together, the resolve of the United States to strengthen its own cybersecurity, coupled with our commitment to uphold norms, is a positive development for the security and resilience of our space systems. Though this section may seem particularly U.S. centric for an organization that operates with space entities on a global scale, a major goal of this paper is to support the proposition that space systems are a U.S. critical infrastructure sector, and thereby covered under U.S. arrangements.

Work has already been done regarding the development of cybersecurity norms for space systems [23]. In general, this work has concluded that norms developed generally for cybersecurity remain nascent and largely unenforced, despite the Paris Call's language regarding the need to *"uphold established global norms in cybersecurity."* Attribution remains uncertain in some cases, barriers to entry for malicious cyber operations remain low, as is the price suffered by our cyber adversaries.

Nonetheless, work on cybersecurity norms is proceeding. Visner and Sharfman note:

> "For some years, an effort has been under way to develop and codify norms to prohibit or limit cyber-attacks in general. The United Nations has convened a "group of governmental experts to deal with ICT threats in the context of international security" that has established five "pillars of work":

- Existing and emerging threats
- International law
- Norms, rules, and principles
- Confidence-building measures
- International cooperation and assistance in capacity-building.

This effort has created a working group representing 193 UN-member countries, and issued a report observing that voluntary, non-binding norms can contribute to conflict prevention. It called on states to avoid using information and communications technology "not in line with the norms for responsible State behavior." In other words, the violation of these norms – still to be defined – would lie outside the bounds of behavior considered acceptable by recognized states" [23].

Nonetheless, cyber attacks against our infrastructures continue. The authors note, however, that attacks against space systems have been rare. They point to norms associated with space systems and recommend that norms associated with the security and resilience of space systems should be built on existing norms, well established, and largely observed, associated with the space domain, rather than emerging and still uncertain norms associated with cybersecurity. Since that paper was published cyber attacks against satellite systems have escalated, particularly in regard to the conflict between Russia and Ukraine.

Given this reality, the Space ISAC recommends the following:

- Pursue the work of the Paris Call to develop cybersecurity norms generally.
- Strengthen the security and resilience of US space systems to reduce the likelihood that attacks and exploits against these systems would be effective.

In addition, adopt the recommendations in [23], as follows:

- Encourage those who deploy commercial space systems to operate them in ways that benefit other countries as well as the United States and call these benefits to everybody's attention.
- Respond to any cyber-attack on a US space system in a way that will strongly discourage any future attacks.
- Engage in informal consultations with those countries that possess substantial space and/or cyber capabilities regarding a possible amendment to Article 7 of the Space Treaty extending its prohibitions on attacking space systems to the use of cyber weapons.
- If these consultations are not productive, issue a unilateral US policy statement that cyber-attacks on space systems are unacceptable.

PILLARS AND GUIDING PRINCIPLES

The Space ISAC is dedicated to creating a broadly useful international framework for information sharing. We utilized the three (3) key pillars below to develop our guiding principles:

1. Space participants (including individuals, companies, nation-states, etc.) should encourage and facilitate the development of acceptable international, interspace, and space community behaviors and norms. We will collaborate with national and international organizations focused on collective security.
2. The evolutions of the space community, like the development of regulated space assets, should be adoptable by the broader space community. Considerations for providers, consumers, and other community members are accounted for, as well as the potential impacts and gains, such that the voices of community members are heard across the global space community.
3. The global space community will have access to a universal public/private information sharing and analysis center (Space ISAC), a community of interest which allows them to reduce the impact of cyber based threats and incidents.

We developed the following guiding principles using our key pillars:

- Key decisions for the global space community should consider the benefits and risks of international engagement with a focus on innovative public-private partnerships.

- Emerging space technology solutions should consider the risks and responsibilities related to space systems, as defined in SPD-5. Reference NIST SP 800-160 [24] and CNSSI 1253 Space Overlay [25] for evolving guidance on resilience.
- Integrated space communities of interest and ideation sessions are considered key elements to foster global alignment to keep pace with the evolving space threat landscape.

CONCLUSION

The official recognition of space as a critical infrastructure is only a matter of time. In today's modern world, it is becoming impossible to conduct regular activities across the globe without the help of our space infrastructure. The Space ISAC, like the White House, sees space as a source of American innovation, opportunity, leadership, and strength. Space activities power our economy and our way of life; spur innovation; inspires us, and helps us manage our resources by protecting people, property, and the environment. In line with the Space Priorities Framework, the Space ISAC supports maintaining a robust and responsible U.S. space enterprise and preserving space for current and future generations. It is our belief that to accomplish these and future priorities, the global space industry must address STEM workforce development needs, research the global climate impacts of space operations, and establish a series of rules and norms for space.

ACKNOWLEDGEMENTS

The Space ISAC would like to thank our members and partners, especially the members of the Information Sharing Working Group, for their contributions to this publication. Special mentions go out to Jeffrey Kaczmarczyk, Samuel S. Visner, Michael Hankins, Tomas Pena, PhD, Peter Sharfman, PhD, and Ian Grahek for their direct participation in the drafting, writing, and development of this white paper.

REFERENCES

[1] The White House: President Joseph R. Biden, Jr., *United States Space Priorities Framework,* Washington, D.C., 2021.

[2] The Space Information Sharing and Analysis Center (Space ISAC), "About Space ISAC," 2019. [Online]. Available: https://s-isac.org/about-us/.

[3] United Nations, *Prevention of an Arms Race in Outer Space: Reducing Space Threats Through Norms, Rules And Principles Of Responsible Behaviors,* vol. A/RES/76/231, 2021.

[4] L. Austin III, *Tenets of Responsible Behavior in Space,* Secretary of Defense.

[5] B. Kennedy, R. Fry and C. Funk, "6 Facts about America's STEM Workforce and Those Training for It," Pew Research Center, 14 April 2021. [Online]. Available: https://www.pewresearch.org/fact-tank/2021/04/14/6-facts-about-americas-stem-workforce-and-those-training-for-it/.

[6] M. D. P. &. P. D. Park, "Early Childhood Teacher's Beliefs About Readiness For Teaching Science, Technology, Engineering, And Mathematics," *Journal of Early Childhood Research,* vol. 15, no. 3, 2017.

[7] National Science Board;, *Revisiting the STEM Workforce: A Companion to Science and Engineering Indicators,* 2015.

[8] The White House: President Joseph R. Biden, Jr., *Interim National Security Strategic Guidance,* 2021.

[9] The White House: President Joseph R. Biden, Jr., "Fact Sheet: Prioritizing Climate in Foreign Policy and National Security," 21 October 2021. [Online]. Available: https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/21/fact-sheet-prioritizing-climate-in-foreign-policy-and-national-security/.

[10] The White House: President Joseph R. Biden, Jr., *Report On The Impact Of Climate Change On Migration,* 2021.

[11] U.S. Department of Defense, Office of the Undersecretary for Policy (Strategy, Plans, and Capabilities), *Department of Defense Climate Risk Analysis,* Report Submitted to National Security Council, 2021.

[12] National Intelligence Council, *Climate Change and International Responses Increasing Challenges to US National Security Through 2040,* NIC-NIE-2021-10030-A, 2021.

[13] U.S. Department of Homeland Security, *DHS Strategic Framework For Addressing Climate Change,* 2021.

[14] United Nations Office for Outer Space Affairs, "The World Space Forum Series," [Online]. Available: https://www.unoosa.org/oosa/en/ourwork/world-space-forum/WSF-main-page.html.

[15] National Aeronautics and Space Administration, "15 U.S.C. Chapter 82 - Land Remote Sensing Policy Act," 3 August 2017. [Online]. Available: https://www.nasa.gov/offices/ogc/commercial/15uscchap82.html.

[16] U.S. Geological Survey , "First Images of Earth Taken by the Landsat 9 Satellite Released," 8 November 2021. [Online]. Available: https://www.usgs.gov/news/featured-story/first-images-earth-taken-landsat-9-satellite-released.

[17] D. Homer, "ESA and SAP on How Business Change Can Slow Climate Change," 30 October 2020. [Online]. Available: https://news.sap.com/2020/10/esa-and-sap-slow-climate-change/?source=social-global-forbes-blog-IEumbrella-2021-NASA.

[18] World Meteorological Organization, "WMO Strategic Plan 2020-30," [Online]. Available: https://public.wmo.int/en/about-us/vision-and-mission.

[19] The International Space Environment Service, "Welcome to the ISES," [Online]. Available: http://www.spaceweather.org/.

[20] M. Borowitz, "Open Space The Global Effort for Open Access to Environmental Satellite Data," MIT Press, 2017.

[21] U.S. Cyberspace Solarium Commission, "NDAA Enacts 25 Recommendations from the Bipartisan Cyberspace Solarium Commission," 2021 National Defense Authorization Act, 2 January 2021. [Online]. Available: https://www.solarium.gov/press-and-news/ndaa-override-press-release.

[22] U.S. Department of State, "The United States Supports the Paris Call for Trust and Security in Cyberspace," 10 November 2021. [Online]. Available: https://www.state.gov/the-united-states-supports-the-paris-call-for-trust-and-security-in-cyberspace/.

[23] S. S. Visner and P. Sharfman, PhD, "Development of Cybersecurity Norms for Space Systems," American Institute of Aeronautics and Astronautics, Inc., https://doi.org/10.2514/6.2021-4050, 2021.

[24] R. Ross, M. McEvilley and J. Oren, "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," *NIST Information Technology Laboratory Computer Security Resource Center,* Vols. SP 800-160 Vol. 1, 2018.

[25] Committee on National Security Systems, *Security Categorization And Control Selection For National Security Systems,* The Committee on National Security Systems (CNSS) Instruction No. 1253, 2014.