CSC 2.0

Time to Designate Space Systems as Critical Infrastructure

By Frank Cilluffo, RADM (Ret.) Mark Montgomery, Sharon Cardash, & Kelsey Shields

Executive Summary

"We're in a space race" with China, NASA Administrator Bill Nelson warned in December.[1] The nature of that race is different from the Cold War contest with the Soviet Union that America fought and won. The national security components of the space race today include not just weapons systems but also the security of critical infrastructure — much of which relies on global positioning satellites, remote imagery, and advanced communication. The economic aspect is just as striking. The Space Foundation, a nonprofit advocacy group, has determined that the global space industry generated $469 billion in revenue in 2021.[2] This number will only increase with technological and manufacturing innovation.

More than a decade ago, the U.S. National Security Space Strategy warned that space will become more "congested, contested, and competitive."[3] This warning proved prescient, but the U.S. government has not done enough to adapt to that reality. Major portions of American space systems are still not designated as critical infrastructure and do not receive the attention or resources such a designation would entail. The majority of today's space systems were developed under the premise that space was a sanctuary from conflict, but this is no longer the case. The threat from Russia and China is growing. Both those authoritarian powers have placed American and partner space systems in their crosshairs, as demonstrated by their testing of anti-satellite (ASAT) capabilities. The United States needs a more concerted and coherent approach to risk management and public-private collaboration regarding space systems infrastructure.

After interviewing more than 30 industry and government experts, the authors have concluded that designating space systems as a U.S. critical infrastructure sector would close current gaps and signal both at home and abroad that space security and resilience is a top priority. In 2013, Presidential Policy Directive-21 (PPD-21) designated 16 critical infrastructure sectors "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."[4] Space systems clearly meet this threshold.

The term "space systems" encompasses the ecosystem from ground to orbit, including sensors and signals, data and payloads, and critical technologies and supply chains.[5] (See Figure 1.) This terminology (which sidesteps the conceptual debates about whether "space" is an infrastructure or only a domain)[6] aligns with presidential Space Policy Directive-5 (SPD-5) of September 2020, which defines space systems to include ground systems, sensor networks, and space vehicles.[7] SPD-5 provided a set of voluntary best practices "to guide and serve as the foundation for the United States Government approach to the cyber protection of space systems." This report seeks to build on these efforts, which constituted an important step toward recognizing and addressing the implications of the nexus between the cyber and space domains.

Time to Designate Space Systems as Critical Infrastructure

By Frank Cilluffo, RADM (Ret.) Mark Montgomery, Sharon Cardash, & Kelsey Shields

Protecting space systems will require an enhanced model of public-private partnership with genuinely shared risk management responsibilities. On the government side, the agency that serves as lead sector risk management agency (SRMA) for this sector will have a demanding task — but one that NASA is well suited to fulfill so long as it receives the extra resources necessary to develop its capacity to protect national security, civil, and commercial systems. There will need to be subgroups within the sector that maintain relationships with other government agencies. One subgroup should deal with defense and intelligence systems, and another with communications systems already regulated by the Federal Communications Commission (FCC). But no alternative candidate for lead SRMA possesses the same range of requisite capabilities as NASA.

Fostering security and resilience in the space systems sector will require mitigating unique cybersecurity challenges that stem from the geographic and technological particularities of space, as well as new and emerging space-based missions. Substantial investment through congressional appropriation will be imperative because policy without resources is merely rhetoric.

---

1. Bryan Bender, "'We better watch out': NASA boss sounds alarm on Chinese moon ambitions," *Politico*, January 1, 2023. (https://www.politico.com/news/2023/01/01/we-better-watch-out-nasa-boss-sounds-alarm-on-chinese-moon-ambitions-00075803)

2. "Space Foundation Releases the Space Report 2022 Q2 Showing Growth of Global Space Economy," *Space Foundation*, July 27, 2022. (https://www.spacefoundation.org/2022/07/27/the-space-report-2022-q2)

3. U.S. Office of the Director of National Intelligence and Department of Defense. "National Security Space Strategy: Unclassified Strategy," January 2011. (https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/2011_nationalsecurityspacestrategy.pdf)

4. The White House, "Presidential Policy Directive -- Critical Infrastructure Security and Resilience," February 12, 2013. (https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil)

5. Historically, however, the phrase "space systems" may have been understood more narrowly.

6. Some contend that space is a domain and only a domain, as opposed to an infrastructure. As a domain, space is like cyber in that both transcend all other domains.

7. The White House, "Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems," September 2020. (https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems)

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.

CSC 2.0 is preserving the legacy and continuing the work of the Cyberspace Solarium Commission For more information, visit **www.CyberSolarium.org**

Time to Designate Space Systems as Critical Infrastructure

By Frank Cilluffo, RADM (Ret.) Mark Montgomery, Sharon Cardash, & Kelsey Shields

Recommendations Summary

For the Executive Branch

Recommendation 1: Designate space systems as a critical infrastructure sector.

1.1 – Designate NASA as the SRMA for the space systems sector.

1.2 – Create two directed subgroups within the sector.

1.3 – Do not assign the SRMA a regulatory role.

1.4 – Articulate and offer industry a clear value proposition.

1.5 – Strengthen international norms and standards.

1.6 – Integrate the National Space Council into the governance of the space systems sector.

For Congress

Recommendation 2: Give NASA, the lead SRMA, the resources to effectively accomplish the mission.

2.1 – Direct the Congressional Research Service to undertake a legislative review.

For Industry

Recommendation 3: Marshal and organize the commercial space community to play an instrumental role in governance.

3.1 – Establish a space systems sector coordinating council (SCC).

3.2 – Task the SCC, through its charter, with working to reduce risks to the security and resilience of the commercial space sector.

3.3 – Leverage and build upon the existing work of Information Sharing and Analysis Centers (ISACs), including the Space ISAC.

For Industry and Government Together

Recommendation 4: Create a co-led risk management enterprise.

4.1 – Jointly elaborate and widely implement cybersecurity best practices.

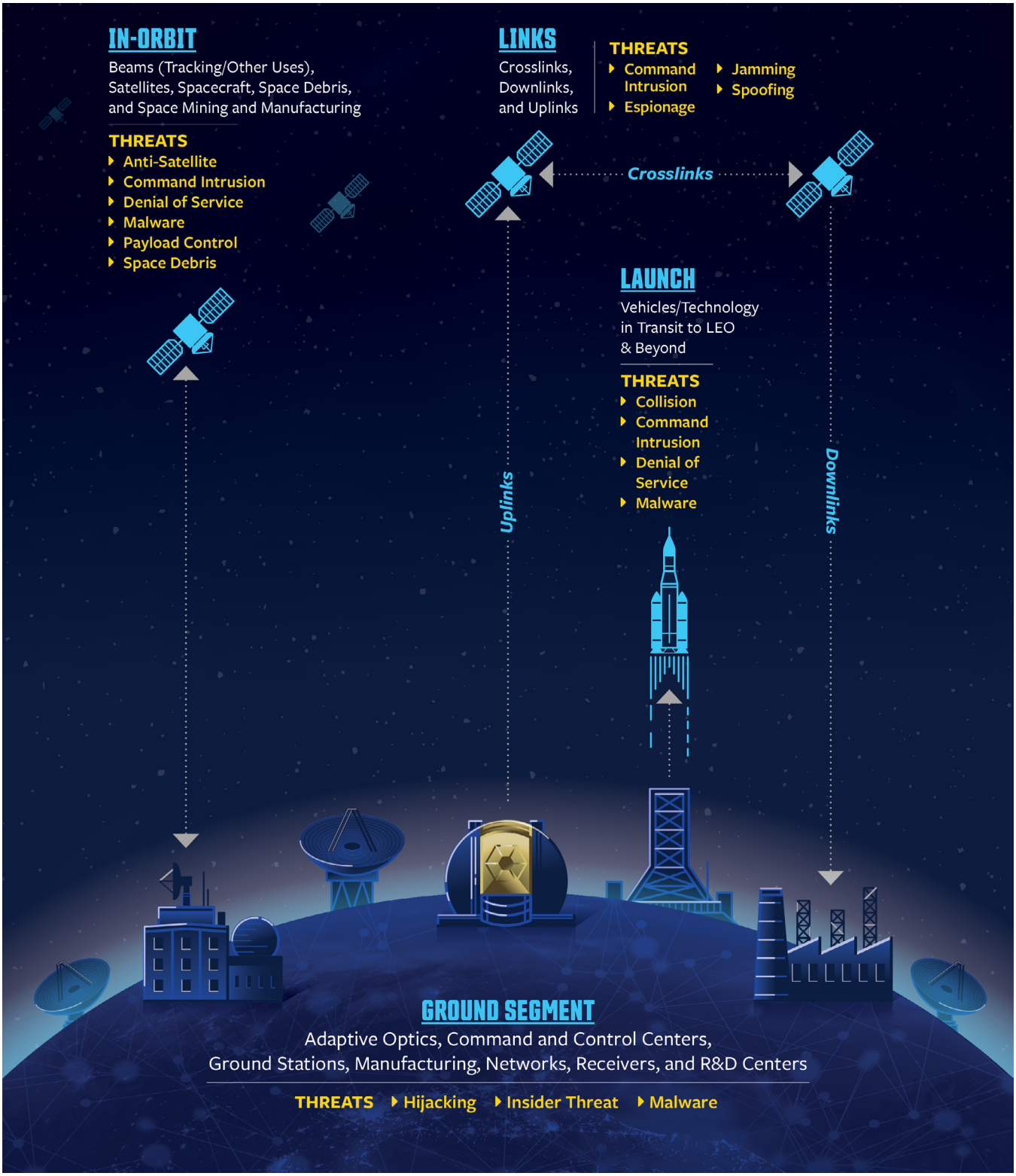
4.2 – Pair commercial and government capabilities to model a dynamic risk environment.

4.3 – Add space assets positioned outside of traditional operational areas to enhance U.S. resilience.

Time to Designate Space Systems as Critical Infrastructure

By Frank Cilluffo, RADM (Ret.) Mark Montgomery, Sharon Cardash, & Kelsey Shields

Figure 1: The space systems threat spectrum



The examples cited above are illustrative and not exhaustive.