Shared Space: Why It is Critical We Collectively Address Security & Resilience in Space

By Megan Moloney and Dan Lewis

This article looks at the need for cybersecurity and risk management efforts to keep up with the rapidly growing importance of space.

Abstract

The strategic and economic importance of space is growing at warp speed. Yet, cybersecurity and supply chain risk management practices for space are wanting. Modernization efforts for both are urgently needed to protect critical infrastructure in space. Moreover, collaborative engagement between nations, betwixt government and commercial entities, and within governments is key the collective defense of peaceful space-faring nations.

Space Is Critical

For years the terrestrial set has reaped the benefits of space advancements, like the innovations leading to baby formula, memory foam, and dustbusters. But space has much broader implications today; people would literally be lost without the global positioning system (GPS) and at the whim of nature without reliable weather forecasting. That reliance is only growing. As of January 2022, 90 nations are operating in space, with commercial sectors reaching parity with - and in some instances exceeding - government capabilities [1]. The notion of a space economy is exploding as commercial space travel scales to widespread availability and policy makers debate lunar mining. Approximately 80% of the $447 billion global space industry is currently commercial. As Navy Rear Admiral Tom Zelibor said during the Space Foundation’s State of Space 2022 event, this is an “era of access and opportunity. [2]” With space increasingly becoming a part of our ordinary lives and economy, cybersecurity and supply chain risk management shortcomings are a notable Achilles’ heel.

Space Systems and Assets Are Vulnerable

Space assets were not historically designed to operate in a contested environment, thus cybersecurity was not prioritized in the way it might be today. Furthermore, governments generally custom-built exquisite space assets to last, meaning once they go up, they stay up for a long time. Given the expense and difficulty of performing on-orbit repairs and updates, this often translates into unmaintainable space assets and introduces considerable vulnerability. Key areas of concern include command link jamming and intrusion, GPS jamming and spoofing, corruption of sensor systems, malicious code injection, and denial-of-service attacks. Each of these concerns presents risk to mission, orbital security, and human safety. A potentially target rich environment presents a pressing national security concern as adversary space capabilities advance and pacing threats become increasingly bold in counterspace operations, threatening to deny, degrade, disrupt, and even destroy national space assets.

U.S. as a Case Study of the Growing Strategic Importance of Space

The strategic importance of space is not lost on U.S. policy makers and the national security apparatus. The Space Force became the first new American service in more than seven decades when it was established in December of 2019 to provide decision makers with additional military options. The Department of Homeland Security launched a Space Systems Critical Infrastructure Working Group in May 2021 to “identify and develop strategies to minimize risks to space systems that support the nation’s critical infrastructure. [3]” In June of 2021, Rep. Ted Liu introduced the Space Infrastructure Act, HR 3713, designed to designate space systems, services, and technology as critical infrastructure. This means that space “systems and assets, whether physical or virtual, [are] 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]” While the determination to
designate space as the 17th critical infrastructure is still being legislated in the United States, entities like the Intelligence and National Security Alliance (INSA) have stated it “would clarify government agencies' roles and responsibilities in protecting space infrastructure, make clear to U.S. adversaries that the United States is committed to defending its space infrastructure, contribute to the establishment of global norms regarding the safety and security of space systems, and accelerate development of best practices and technologies for ensuring cybersecurity and resilience of space assets. [5]” Further signaling the strategic importance of space, the Biden Administration resuscitated the National Space Council in December 2021 under Executive Order 14056, directing it to “synchronize the Nation’s civil, commercial, and national security space activities in furtherance of the objectives of the President’s national space policy and strategy” and “enable interagency cooperation, coordination, and information exchange on space activities. [6]”

There is a Parallel U.S. Policy Evolution to Protect Space Assets

Over the past few years there has been a steady demand signal for more robust policy and international norms in space. In December 2020, the White House released a Memorandum on National Space Policy which sets forth as one of its primary goals to “[c]reate a safe, stable, secure, and sustainable environment for space activities, in collaboration with industry and international partners, through the development and promotion of responsible behaviors; improved practices for the collection and sharing of information on space objects; protection of critical space systems and supporting infrastructures, with special attention to cybersecurity and supply chains; and measures to mitigate orbital debris.” Similarly, the United States Space Priorities Memorandum published in December 2021 sets forth that “the United States will work with the commercial space industry and other non-governmental space developers and operators to improve the cybersecurity of space systems, ensure efficient spectrum access, and strengthen the resilience of supply chains across the nation’s space industrial base.” Key themes that arise from these strategy and policy documents include: commercial use, collaboration, cybersecurity, and resilience. Each of these is seen as essential to maintaining U.S. overmatch in the space domain.

Commercial Use

It widely acknowledged that embracing commercial use will help to drive innovation, rapid acquisition, and modular building to modernize the approach to space. In 2018, the Trump Administration issued Space Policy Directive 2, “Streamlining Regulations on Commercial Use of Space,” which called for a review and easing of commercial use regulations pertaining to launch and re-entry licensing, commercial remote sensing, radio frequency spectrum, and export licensing [7]. In the time since, commercial-first policies have been implemented by entities like the U.S. Space Force, Space Development Agency, and the National Aeronautics and Space Administration [8]. Summarizing and further driving this trend, the 2020 National Space Policy states: “A robust, innovative, and competitive commercial space sector is the source of continued progress and sustained United States leadership in space. [9]”

Cybersecurity

The first comprehensive cybersecurity policy for space systems, Space Policy Directive 5 (SPD-5) [10], was published in September 2020 to address these concerns and provide guidance on the protection of space assets. While it recognizes that the same security principles applied to terrestrial systems should extend to space systems, it notes that the unique nature of space systems elevates certain principles and practices, such as the ability to perform updates and respond to incidents remotely. Specifically, SPD-5 lays out the following five principles:

- Space systems [11] and infrastructure (to include software) should be developed using risk-based, cybersecurity-informed engineering (to include continuous monitoring);
- Space systems must have cybersecurity plans that ensure the confidentiality, integrity, and accessibility of critical functions, to include protecting against unauthorized access, minimizing command, control and telemetry system vulnerabilities, guarding against communication jamming and spoofing, managing risks to the supply chain, and generally driving better cyber hygiene;
- Best practices and norms of behavior should be integrated into space system requirements and governing rules, regulations, and guidance;
- Collaboration and information-sharing across government and commercial owners and operators is essential; and
- Space system owners and operators should take effective cybersecurity measures but may manage their own risk tolerance, balancing security against mission requirements to minimize undue burden.

Resilience

According to Gen. John “Jay” Raymond, Chief of Space Operations, United States Space Force, resiliency will be a key focus in 2022. “We have got to shift our space architecture... from a handful of exquisite capabilities that are very hard to defend to a more robust, more resilient architecture.” While this includes the deployment of proliferated satellite constellations and improved propulsion systems, [12] it also means taking a hard look at the supply chain. Not only is it necessary to have the ability to supply the parts needed to build next generation capabilities, but also to advance then from the ground with new software and hardware. The integrity of that software and hardware will be critical to the security and resilience of “birds” in flight.

Collaboration

Information sharing may sound like a soft requirement at first blush to newcomers to the space domain, but there is a reason it is called for in nearly every strategy and policy document of consequence related to space: it is essential for safe and sustainable space operations. This has always been true, but its import...
has been elevated in light of the recent development, launch, and aggressive testing of anti-satellite weapons by both China and Russia. This not only poses a militaristic threat to space assets, but also subjects them to the significant hazard of space debris. For example, the 15 November 2022 direct-assent anti-satellite weapon test by Russia resulted in as many as 1,500 new pieces of space debris that put astronauts in the International Space Station on high alert.[13] International consensus about space norms is needed in addition to improved information sharing about potential vulnerabilities, threats, and intrusions.

**Immediate Actions to Enhance Security and Resilience in Space**

Although the regulatory framework and policy evolution above is specific to the U.S., the themes are not. Nor are the actions that can be taken to enhance resilience and security in space. In fact, the actions highlighted below must be taken to enhance the collective defense of peaceful space-faring nations.

**Reduce Barrier to Entry for Non-Traditional Actors**

The defense industrial base supporting space has traditionally been a handful of large-scale companies developing and launching exquisite space assets, but there is an acknowledged need to diversify the market and invite smaller, non-traditional companies to bring greater innovation and speed development in the space domain. In order for that to be feasible, the barriers to entry must be lowered. There are a variety of ways to achieve that, a number of which are already underway. Contracting policies and practices must be reworked to become more open and flexible to drive rapid acquisition. U.S. entities such as the Space Enterprise Consortium and the Defense Innovation Unit have prioritized this endeavor and are already making significant headway bringing non-traditional partners to the table. Similarly, in order to meet the speed of the threat, the space industry is transitioning to smaller and modularly built assets. Nanosatellites provide a broader attack surface and greater resilience, but also allow for companies to enter the market with less investment. Modular building allows non-traditional companies that specialize in one portion of the design, build, launch, or operation of space assets to win work while simultaneously creating a build paradigm that can respond more effectively to and cordon off negative cascading effects of defects and compromise.

**Extend Risk-Based Approach to All Space Cybersecurity**

Given that cybersecurity was not historically prioritized in the design, build, launch, and operation of space assets, it is urgent that the community elevate it. That said, it won’t happen overnight, especially as increased commercial use introduces a plethora of new non-traditional small businesses. A risk-based approach to cybersecurity in the space domain is required in this era of great power competition. Geared towards risk reduction, a risk-based approach is a pragmatic way to identify, prioritize, and address the most significant cybersecurity vulnerabilities and threats. This approach has gained favor for terrestrial cybersecurity. For example, the Strengthening American Cybersecurity Act legislative package that was recently approved by the U.S. Senate would require federal agencies to adopt a risk-based approach and improve coordination amongst themselves. As for the space domain, SPD-5 specifically calls for space systems and infrastructure to be developed using risk-based, cybersecurity-informed engineering, but that should be extended throughout the lifecycle of space assets. Moreover, cascading policies and business processes must be updated to reflect and implement this imperative.

**Modernize Supply Chain Risk Management Practices**

Just as cybersecurity approaches must be reassessed to accommodate burgeoning commercial use, so must supply chain risk management practices. Supply chain practices have often been siloed in specific parts of an organization, concentrating on pre-procurement vendor review for major acquisitions. This approach is ill-designed to address the threat, particularly as it relates to cyber, and compounds the vulnerability of today’s space assets. Space owners and operators must take a holistic approach to supply chain risk management, building enterprise-wide programs that assess and assign prioritization to risks for all critical acquisitions cradle to grave. Furthermore, supply chain risk management programs of the future must take a more proactive stance, leveraging diverse skills, tools, and technology to research, understand, and address evolving and emerging threats. This will entail a far more agile approach in terms of program strategy and staffing.

**Collaborate as if the Future Depends Upon It**

Collaborative engagement between nations, betwixt government and commercial entities, and within governments is key to both cybersecurity and resilience. Improved information sharing about vulnerabilities, threats, and incidents is necessary to protect international space assets in an increasingly congested and contested environment. Leveraging existing entities, such as the Space Information Sharing and Analysis Center, will advance meaningful crosstalk in this regard. Global consensus is urgently needed in light of aggressive anti-satellite capability demonstrations and consequential space debris, with experts calling for an international Space Summit. There is also need for more formal and informal governmental avenues to build strong trust and transparency between space owners and operators. As proposed in the 2021 State of Space Industrial Base Report, the U.S. would benefit from a “National Space Enterprise Task Force to serve as an interagency coordinating body, synthesizing diverse perspectives and rapidly resolving space-related issues across participating departments and agencies. [14]” Similarly, there is a need for a place where government entities can have an informal dialogue to share best practices and lessons learned to drive program maturity.
Conclusion

Gen. Jay Raymond plainly stated "[o]ur security and resilience in space is critical for our democracy-based world order in the future. [15]" As highlighted in the 2021 State of the Space Industrial Base report, advantage begets advantage under the Matthew Principle. [16] In order for peaceful space-faring nations to maintain advantage in space, they must embrace and innovate with commercial partners, secure our cyber infrastructure and supply chains, and collaborate as if the future depends on it.

References

11. “Space System’ means a combination of systems, to include ground systems, sensor networks, and one or more space vehicles, that provides a space-based service. A space system typically has three segments: a ground control network, a space vehicle, and a user or mission network. These systems include Government national security space systems, Government civil space systems, and private space systems.” Space Policy Directive-5 (2)(a) (September 2020).

About the Authors

Megan Moloney brings two decades of legal, investigative, intelligence, and risk management experience to help clients develop forward-leaning strategy, build meaningful collaboration, and tackle the hard problems. She is passionate about enhancing the preparedness and resilience of the U.S. national security apparatus. Currently, she is concentrating on maturing federal supply chain programs and strengthening collective defense.

Daniel Lewis is a Director in Guidehouse lead Cybersecurity and Information Security efforts across its National Security Segment. Over the last 13 years, he has supported the identification and resolution of risks to space programs and mission systems across the Intelligence and Defense communities in order to strengthen our Nation’s cyber posture and resiliency.