

Science & Technology Innovation Program



Wilson
Center



Science and Technology
Innovation Program

Image source: [By ktsdesign / Shutterstock.com](#)

Authors

Melissa K. Griffith

*Senior Program Associate,
The Woodrow Wilson
International Center for
Scholars*

Christopher M. Hocking

*Lieutenant Colonel,
U.S. Air Force*

Seizing Opportunities: Four National Security Questions to Ask About the Use of Satellites in 5G Networks

September 2021





Acknowledgements

As a contribution to two initiatives (The Wilson Center’s **5G Beyond Borders** and the Science and Technology Innovation Program’s **Across Karman**), this policy brief addresses three pressing national security concerns related to critical infrastructure protection: space, telecommunications, and cybersecurity. Special thanks go to the Science and Technology Innovation Program (STIP) and to Meg King, Elizabeth Newbury, and Sophie Goguichvili for their feedback and comments throughout the editing process. We also owe a debt of gratitude to Eric Burger, Jennifer Manner, Bryan Tipton, and the many individuals who shared their experiences, expertise, and insights with us over the course of this project.

Executive Summary

In order to deliver on the full promise of the fifth generation of mobile (5G) networks (near ubiquitous, instantaneous coverage for a massive number of connected devices), satellites will need to play a far more central role within telecommunications networks going forward with both terrestrial and space-based components working in tandem for a wider diversity of functions. Given the evolution of the satellite industry, both in terms of business models and technology, that greater role is now increasingly possible. Yet, while much of the focus on the national security implications of 5G to date in the United States and abroad has been on the terrestrial components of these networks (e.g. Internet of Things (IoT) and mobile devices, radio heads and towers, fiber, the core network, etc.), the potential role of satellite communications systems in these networks has been largely overlooked and/or poorly misunderstood. What steps, therefore, should we prioritize today to ensure greater security and resilience of 5G networks now and in the future? Put another way: if you are a policy maker concerned with the potential data-centric national security risks associated with reliance on satellite segments by 5G telecommunications networks, what questions should you ask and why do the answers to those questions matter?



TABLE OF CONTENTS

Introduction	4
5G and National Security: Why Worry?	7
The Role of Satellites in 5G Networks	8
When We Say “Satellites,” What Do We Mean?	9
How Has the Role of Satellites in Telecommunications Networks Evolved Over Time?	11
What Purpose Could Satellites Serve in 5G Networks?	16
Satellites, the (Not So) Novel Critical Infrastructure Problem	18
Worried? Four Questions to Ask	20
Q1 - Criticality: Who Depends on a Particular Satellite System (Now and in the Future), to What Degree, and for What Purposes?	21
Q2 - Physical Architecture: What Does the Ground Teleport Infrastructure and Launch Capabilities Look Like, and Where Are They Located?	24
Q3 - Data and Digital Systems: How Does the System Protect the Data It Is Moving and Ensure That the Data Keeps Moving Reliably?	27
Q4 - Supply Chains: Which, and How Many, Vendors Comprise the Satellite System’s (Hardware and Software) Supply Chain?	31
Conclusion	33
About the Authors	35
References	36



Introduction

For the promise of the fifth generation of mobile networks (5G) to be fully realized (i.e. nearly ubiquitous, instantaneous, connectivity for large numbers of devices globally), terrestrial telecommunications systems, which heavily rely on buried fiber optic cables, will not be enough.¹

Instead, we will need to move from (a) largely separate satellite and terrestrial communications systems with satellites used primarily for solving “the last mile” problem (areas where laying fiber was a physical or economic challenge) or for discrete use cases (e.g. processing credit card payments at a gas station) to (b) an integrated 5G ‘network of networks’ where satellites play an increasing role alongside terrestrial networks.

Why is 5G Important?

“5G is a core foundation upon which modern societies—their economies and their militaries alike—will rest. [This network of networks] will be essential to how industries compete and generate value, how people communicate and interact, and how militaries pursue security for their citizenry. 5G is potentially one of the most important networks of the 21st century. It is the very definition of critical infrastructure.”—excerpt from “[5G and Security: There is More to Worry about than Huawei](#)” (Griffith, 2019)

Why? While the utility of satellite communications is more limited within cities and in city-to-city communications (areas where fiber and WIFI already dominate and the lines of sight necessary for satellites are significantly reduced), integrating satellite and terrestrial systems will be necessary to meet the full spectrum of future demands likely to be placed on 5G networks. These include

1. increasing traffic and number of connections outside of dense city centers in more rural and remote areas with the proliferation of Internet of Things (IoT) devices,
2. providing coverage for devices on the move (such as a ship at sea or a car driving across the United States), and
3. processing and data caching pushing progressively closer and closer to the networks’ edge (i.e. edge computing)² and farther away from areas of dense fiber availability.

1 The exact ratio between terrestrial and satellite systems needed to realize the full potential of 5G remains an open question. The answer will depend on a variety of factors including government incentives (e.g. infrastructure support to lay fiber), the business models that are emerging and continue to evolve in the satellite space, the preferences of (or business decisions undertaken by) network providers, the market dynamics of and existing infrastructure in the area (ratios will differ by locality as well as country to country), the evolution and demands of use cases (many 5G use cases have not yet been fully realized or imagined), etc.

2 Edge computing reduces latency by bringing compute and storage capabilities closer to the end-user (their devices and applications). This migration of functionality is achieved by leveraging cloud computing models and other innovations in the radio access network (RAN) to shift computing applications within or to the boundary of an operator’s network.



Take, for example, the connectivity needs of mobility. If you disconnect a mobile asset (car, truck, plane, drone, ship) from the fiber network, you can still keep it connected by WIFI and terrestrial 5G infrastructure so long as it is in or is in close proximity to cities. But as you move to more rural and remote areas, only satellite communication (SATCOM) has the potential to provide reliable coverage and sufficient data density. As the number, uses, and requirements of connectivity continue to evolve, so does the importance of extending the promise of 5G networks beyond the urban and densely networked communities.

To meet these demands, satellites will need to serve a diversity of purposes ranging from the “last mile” problem to connections on the move, redundancy for critical emergency services, edge networking, and IoT dense traffic areas outside of the already highly networked cities.

In short, satellites will play a key role in determining our collective 5G future. How we integrate terrestrial and space-based components will determine the type and degree of connectivity 5G networks enable in practice across the United States and around the world, rather than what they could have enabled in theory.

As a consequence, 5G represents more than just an important shift in (a) the possibilities for, (b) functions of, and (c) the hardware-software interplay in mobile telecommunications networks as we moved from legacy generations such as 3G

and more modern generations like 4G LTE and now to 5G. 5G also represents an opportunity for a shift in the relationship between terrestrial and space-based communications systems more broadly.

And, importantly, for the first time, an evolution of the underpinning technology (primarily satellite and launch technology) and the business models of satellite companies (including satellites systems as a service) makes this integration both technically possible and economically feasible.

This shift can be seen today by the emergence of companies like SpaceX, OneWeb, AST SpaceMobile, and Project Kuiper, who seek to create disruptive business models in low earth orbit (LEO), as well as more traditional geosynchronous (GSO) providers like Telesat and ViaSat who are adapting their infrastructure and satellite capabilities to compete for market share with the proliferated LEO providers.

As the number, uses, and requirements of connectivity continue to evolve, so does the importance of extending the promise of 5G networks beyond the urban and densely networked communities.

A Diversity of Business Models

Notably, there are a diversity of business models emerging in this space. SpaceX features a consumer-focused broadband service with Starlink, AST & Science has specialized in satellite-to-smartphone with AST SpaceMobile, OneWeb and Telesat offer enterprise-focused networks, AWS Ground Station provides ground stations as a service to support customers’ satellites in orbit, and Lockheed Martin and Omnispace have focused their efforts on developing a hybrid network for both commercial and government customers.



This convergence between terrestrial and space-based telecommunications networks for 5G is not merely hypothetical. Earlier this year (2021), Lockheed Martin’s space division announced a strategic partnership with satellite start-up Omnispace to jointly build out a space-based 5G network. [Their hybrid network](#) seeks to combine satellite and mobile wireless carrier networks to create “a global 5G network, which enables users to seamlessly transition between the satellite [and the] terrestrial network” (Sheetz, 2021). Notably, this hybrid network would be the [first integrated 5G platform for commercial and government use](#) featuring space-based and terrestrial network architectures (“Lockheed Martin and Omnispace Explore Space-Based 5G Global Network,” 2021).

Taken together, these three factors - (i) evolving satellite system technology and (ii) business models coupled with (iii) growing demand for bandwidth - make it possible (though [not inevitable](#)) for satellites to have an increasing role in telecommunications networks in general and 5G networks in particular (Daehnick, Klinghoffer, & Wiseman, 2020).

5G represents an opportunity for a shift in the relationship between terrestrial and space-based communications systems more broadly.

Yet, much of our focus on the national security implications of 5G to date in the United States and abroad has been on the terrestrial components of these networks: IoT and mobile devices, radio heads and towers, fiber, the core network, etc. While 5G is best understood as a ‘network of networks’, many have overlooked or are unaware that such a network of networks can, and should, include

satellites. As such, for those of us concerned with addressing national security concerns associated with this [critical infrastructure](#) now and in the future, satellite systems require additional attention and scrutiny (Griffith, 2019).

Given their potential role as [“one of the most important networks of the 21st century”](#) and [“the very definition of critical infrastructure,”](#) we can no longer afford to focus our attention solely on building satellites that can survive launch, initial operations, and a long life cycle in an hostile physical environment (Griffith, 2019). The security, resilience, and defensibility of these systems against potential malicious actors over time is of equal import. Given that adversaries, or peer competitors, [increasingly view space as a domain of conflict](#) and that our communications critical infrastructure (like 5G) will rely on satellites, the dependability of these systems (both in terms of their continued functioning and the confidentiality, integrity, and availability of data traversing these systems) in the face of potential malicious activity can no longer afford to be an afterthought or absent from our broader critical infrastructure conversations (“Challenges to Security in Space,” 2019).

Looking for a Primer on 5G?

For additional information and resources on 5G networks, refer to [5G.wilsoncenter.org](https://www.wilsoncenter.org/5g). There you can find an overview of 5G networks as well as deeper dives in to the global and North American state of play, technical standards such as Open RAN, and the relationship between 5G networks and great power competition.



Yet, [legacy satellite systems are notoriously insecure](#) (King & Goguichvili, 2020). Many of the system busses³ used over the past decades were products of a focus on surviving the rigors of space—not oriented around the pervasive cybersecurity threats we face today and will face in the future. Due to launch costs, traditional satellites were, and still are, designed for exceptional resilience and survivability in the most unforgiving environment known to humans over long periods of time. This drove the prioritization of redundancy, continued performance despite planned hardware degradation, and other space-unique design considerations over all else. However, even in [newer](#) satellite systems, security can often be an afterthought, and a limited one at that, rather than baked into the initial design, deployment, and maintenance of these systems (Bailey et al., 2019).

...if you are a policy maker concerned with the potential data-centric national security risks associated with reliance on satellite segments by 5G telecommunications networks, what questions should you ask and why do the answers to those questions matter?

What steps, therefore, should we prioritize today to ensure greater security and resilience of 5G networks—their terrestrial and space-based architectures—now and in the future?

Put another way: if you are a policy maker concerned with the potential data-centric national security risks associated with reliance on satellite segments by 5G telecommunications networks, what questions should you ask and why do the answers to those questions matter?

This publication serves two functions. First, we provide an overview for the shifting role of satellites within mobile telecommunication, including how this shift is possible today and why it is necessary. We then provide a basic framework for stakeholders of all sorts to ask questions of the security, operations, and infrastructure of nascent 5G networks and the satellite systems that support them as 5G drives hyperconvergence of telecommunications, satellite communications, and cloud computing.

5G and National Security: Why Worry?

Why should the United States care about the reliability and security of 5G networks, including satellite components of these networks? The short answer: 5G is the critical infrastructure of the future and increasingly the critical infrastructure of the now.

More specifically: while communications serve an “enabling function” for other critical infrastructure and services, given the transformative functions of 5G networks and the use-cases these functions will facilitate, telecommunications will, become even more foundational to the daily operations of governments, companies, and societies. In short, 5G networks will only increase the scale and character of that “enabling function.”

As discussed in more detail in a previous STIP policy brief entitled “[Balancing the Promise and the Peril of 5G: The State of Play in the United States](#)” (Griffith, 2021a):

³ Satellites are comprised of a payload and a bus. The payload is mission specific and differs from satellite to satellite (i.e. the equipment necessary to perform its specific purpose such as communications). The bus provides the essential functionality (i.e. electrical power, electronics, and propulsion) enabling the mission payload.



Threats to critical infrastructure in general, and communications in particular, are not merely theoretical. From the vantage of national security, these sectors can fall victim to two broad categories of malicious operations: espionage operations and disruptive or destructive operations. Espionage operations focus on the gathering of intelligence but not the interruption or destruction of infrastructure. In other words, these types of operations undermine the confidentiality of data within systems but not the integrity or availability of those systems. Espionage operations have long targeted communications networks as a treasure trove of information. Looking to 5G in particular, big data found traversing these networks represents an appealing opportunity for intelligence gathering and intellectual property (IP) theft.

In contrast, disruptive operations seek to undermine the integrity and availability by either temporarily incapacitating systems or destroying them altogether. Disruptions of 5G networks have the potential not only to cripple a hospital's traditional communications systems, but also terminate or introduce potentially deadly lag times into a remote-access surgery in the middle of an operation. Factory floors, leveraging a myriad of connected devices and sensors for manufacturing, could grind to a halt and their corresponding safety-critical systems (e.g. safety instrumented systems (SIS)) could be manipulated into unsafe states. In a world of fully automated cars, sudden increases in latency can lead to physical crashes. Ultimately, given the importance of reliability, speed, low latency, and IoT for 5G use-cases, small disruptions in 5G networks could have outsized impacts on the cyber-physical systems they support.

Notably, the topic of this paper – the satellite communications components of 5G networks – sits at the nexus of not one but two “critical enablers”: telecommunications and space (in this case, the emerging regime of proliferated LEO satellite) systems. Much of the world's critical infrastructure, including communications, is heavily dependent on space (such as [GPS](#)) for its daily functioning and communications is no exception (“Protecting America's Global Positioning System”). A [2013 BBC article by Richard Hollingham](#) strikingly demonstrates this point by reflecting on what would happen if all satellites stopped working: a hypothetical “day without satellites” (Hollingham). This dependency on satellite systems is only likely to increase with the development and deployment of 5G networks and the evolution of the satellite industry (both in terms of the underlying technology and the evolving business models).

5G is the critical infrastructure of the future and increasingly the critical infrastructure of the now.

This makes actively mitigating national security risks related to 5G networks that may emanate from or target communication satellite systems a national security imperative for the United States. To effectively assess current and future efforts in this area, however, requires a nuanced understanding of the evolving role of satellites in 5G networks.

The Role of Satellites in 5G Networks

What are the components of a communication satellite system? Given those components, how have these systems evolved over time? Given that evolution, why are we likely to see a transition away from largely discrete telecommunications systems (terrestrial vs. satellite) toward a more integrated network architecture as we build out and seek to fully leverage 5G networks?



When We Say “Satellites”, What Do We Mean?

‘Satellites’ is often used as shorthand for satellite systems. Satellite systems consist of four basic segments: ground-based assets, space-based assets, links between elements (i.e. uplinks, downlinks, and crosslinks), and connection points to other networks or devices (the users or customers of these systems).

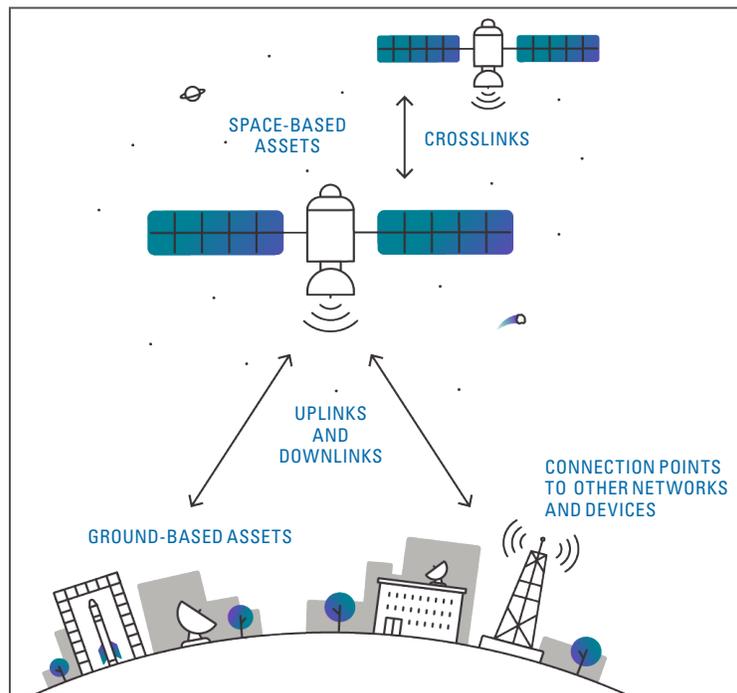


Figure 1. Anatomy of a satellite system.

Ground-based assets are terrestrial (surface-based facilities) and include ground stations and launch facilities. Launch facilities make it possible to put a satellite into space and are historically operated by a company that is distinct from those operating the satellites in practice. Ground stations are the brain of the entire satellite networks. They serve as control systems for the satellites in orbit and, as a consequence, if something goes wrong with a satellite in space, the personnel at these stations will be the first to know and in the best position to carry out incident response. These stations provide real-time communications with satellites enabling telemetry, tracking, and control (TT&C) over satellite networks as well as managing **uplinks** (sending radio signals to the satellite) and **downlinks** (receiving data transmission from the satellite). When people hear satellite systems, it is often the satellite that stands out and tends to garner the most attention. However, these satellites are only effective if they have somewhere to send and act on their data (i.e. ground-based assets). This command and control function is why the [Space Security Challenge’s 2020 Hack-A-Sat](#) focused on regaining control of a compromised satellite from the ground station (“Hack-A-Sat”).

Space-based assets include communication satellites (e.g. to support 5G networks) but also other types of satellite that support systems such as positioning, navigation, and timing (PNT) (supports GPS, EU’s Galileo, Russian GLONAS) and weather satellites. Communication satellites, and satellites in general, are comprised of a payload and a bus. The payload is mission specific and differs from satellite to satellite (i.e. the equipment necessary to perform



its specific purpose, such as communications). The bus provides the essential functionality (i.e. electrical power, electronics, and propulsion) enabling the mission payload. In the context of communications satellites, the mission payload is the communications package including antenna, content/data routing, and waveform management. In addition to uplinks and downlinks between the satellite and the ground station, some satellite constellations can also communicate with each other (**crosslinks**).

Satellite systems are not an island in and unto themselves. Their utility is in their ability to connect with their users. **Connection points to other networks and devices** can take many forms. In the case of serving as 5G backhaul, for example, satellite systems would connect the Radio Access Network (RAN) to the core network.⁴ Both of those connections (the RAN and core) are endpoints for the satellite system. In the case of increasing connectivity for IoT devices in an urban area, numerous IoT devices become endpoints that also need to be managed and where insecurity can be introduced into the satellite system. Notably, communication satellites can support commercial, government, or military purposes and often satellites can support multiple communities at the same time. For example, according to a [DoD study](#), “commercial communications satellites were used in 45 percent of all communications between the United States and the Persian Gulf region during Desert Shield/Desert Storm” (“Critical Infrastructure Protection: Commercial Satellite Security Should be More Fully Addressed,” 2002a).

As an industry, satellite systems are supported by a diverse set of players across the hardware and software supply chain. As summarized in a [2002 GAO report](#) on Critical Infrastructure Protection for commercial satellite systems (“Critical Infrastructure Protection: Commercial Satellite Security Should be More Fully Addressed,” 2002b):

[t]he commercial satellite industry includes manufacturers, the launch industry, service providers, and ground equipment manufacturers. Manufacturers design and build satellites, supporting systems, and ground stations. The launch industry uses launch vehicles, powered by rocket engines, to place satellites in orbit. Once commercial satellites are in orbit, they are operated by service providers, who lease available services.

Now, two decades later, the industry has evolved to also include vertically integrated providers - such as SpaceX, which currently produces everything on the operations side, from their rockets to software for their satellites, in house⁵ - as well as a diversity of users relying on these systems for their connectivity needs as service prices dropped with the emergence of smaller satellites and CubeSat technology, which spreads the cost of a launch across many users.

In short, the communication satellite industry ecosystem is composed of and supported by an array of vendors, operators, and users. Those vendors and operators span ground-based assets, space-based assets, links between the two, and connection points to other networks and devices (the customers). For the fifth generation of telecommunications, that ecosystem will be increasingly integrated with the territorial networks that frequently come to mind when someone says 5G - cellular towers; radio heads; fiber; servers; sensors in cars, hospitals, and factories; a plethora of mobile devices; etc.—and their supporting ecosystems.

4 For a detailed explanation of the components of a 5G network, refer to Balancing the Peril and Promise at <https://5g.wilsoncenter.org/publication/balancing-promise-and-peril-5g-state-play-united-states>.

5 SpaceX currently makes almost everything in-house rather than buy on the operations side (which is separate from the corporate side of the company, such as accounting, word processing, email, etc.). However, that make-buy decision has not leaned toward make simply for the sake of making things in-house. It is the result of SpaceX producing more of these various technologies (at the hardware and software layers) than anyone else for the kinds of use cases they need them for. They change those technologies more often than anyone is used to, and a lot of it is novel in the first place. As a result, from a business perspective, it currently makes more sense to build in-house than to buy from elsewhere. However, if any of those factors changed, the subsequent make-buy decision could change as well.



How has the Role of Satellites in Telecommunications Networks Evolved over Time?

Historically, satellite and terrestrial communications networks developed separately and were largely isolated from each other. Satellites have been used for backhaul in telecommunications networks for almost 30 years. However, while satellites offered significant bandwidth capacity (upwards of 1GB/s), the latency was extremely high, and required extensive physical infrastructure to move data. This meant that any high bandwidth data movement was a (i) costly, (ii) highly orchestrated, and (iii) deliberately planned activity. As a result, satellites have been a critical component for solving the “last mile” problem but, at the same time, largely limited to transmitting data to these disconnected or hard to reach locations.

Why the “last mile”? Most of those satellites sat in geosynchronous earth orbit (GSO) in earth-faced fixed inclination at roughly 36,000 kilometers above the earth. Put simply, if one is placed overhead, look up and it is always overhead and pointing down at you. The benefit of GSO orbit is that their fixed position allows for continuous coverage of a geographic area by matching the rotation of the earth. Given their altitude, a single GSO satellite also has a potentially wide field of view (or coverage area). AT&T’s DirectTV and HughesNET constellations are modern examples of GSO constellation satellite systems. These are large traditional communications satellites (in fact, many of them have their own Wikipedia pages). Importantly, however, these GSO constellations, in general, require professional installation for the customer-facing ground element and offer limited bandwidth. The fixed nature of GEOs is also one of their downsides; given their distance from the earth’s surface, GSOs tend to take longer to transmit data to and from ground-stations and devices than other closer terrestrial transmission stations. While this difference is measured in milliseconds and seconds, it creates challenges when high bandwidth, low latency connections are necessary.

Putting Orbits in Context

Low Earth Orbit (LEO), orbital period of 128 minutes or less and an altitude of less than 2,000 km. Primarily used for communications and remote sensing satellites; the International Space Station and the Hubble Space Telescope are in LEO.

Medium Earth Orbit (MEO), orbital period of less than 24 hours but more than 128 minutes, altitude between 2,000 km and 35,786 km. Primarily used for navigation and timing satellites; GPS and Glonass are in MEO.

Geosynchronous Orbit (GSO), orbital period equal to the earth rotational period, altitude of 35,786 km at fixed longitudinal position. Primarily used for communication and earth sensing satellites; legacy space-based internet satellites and communicates satellites are in GSO.

Geostationary Orbit (GEO), a form of GSO, satellites in GEO specifically orbit the Earth’s equator and appear stationary to an earth observer. Primarily used for communication and earth sensing satellites; satellite TV and weather satellites are in GEO.

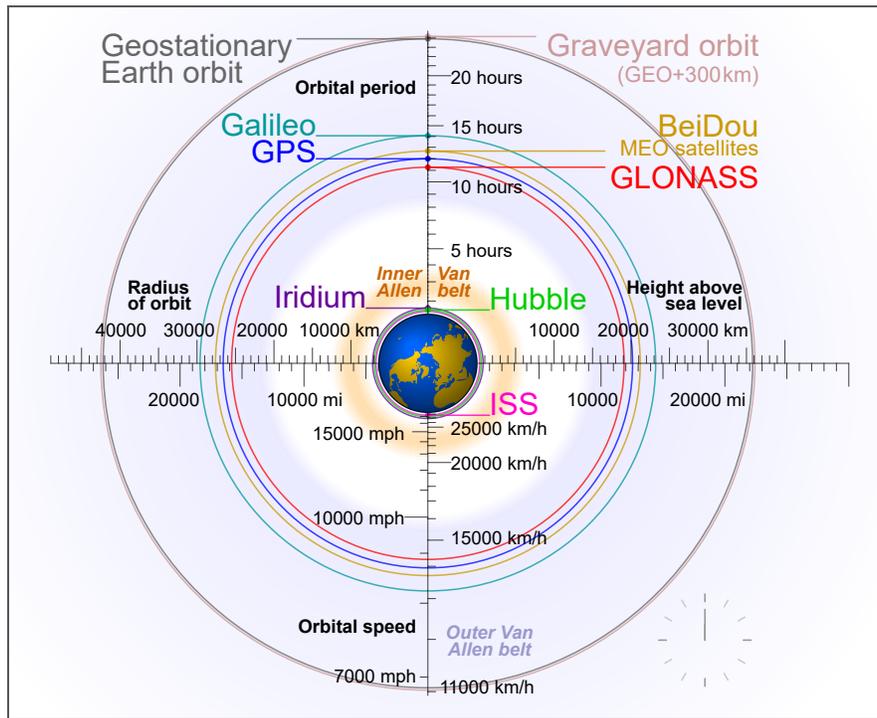


Figure 2. Comparison of GPS, GLONASS, Galileo and COMPASS (medium Earth orbit satellites) orbits with International Space Station, Hubble Space Telescope, geostationary and graveyard orbits, and the nominal size of the Earth. Source: By cmglee - Own work, CC BY-SA 3.0.

What's changed? In contrast to GSO satellites, non-geosynchronous orbit (NGSO) communications satellites, including low earth orbit (LEO) satellites and the particular class of emerging proliferated LEO systems like SpaceX's Starlink constellation, are well positioned to solve more than the "last mile" problem. Unlike traditional LEO and GSO constellations, which have a small number of satellites, **less than 100 in each system**,⁶ the proliferated LEO (pLEO) systems, like SpaceX's Starlink currently have closer to **1,320** and plan to have **several thousand** ("USC Satellite Database," 2021, and Thompson, 2021).

LEOs differ from GSOs in two important ways. First, a LEO typically sits somewhere between **160 and 2000 kilometers** above the earth's surface and these satellites fly in rapid orbits around the earth (many different orbits around the earth at various altitudes – a swarm) ("Low Earth orbit," 2020). Put simply, with pLEOs, a specific satellite is not overhead all the time, but given their speed and numbers, the satellite constellation will be overhead constantly. Second, LEOs, given their low earth orbit, stay in orbit for a shorter period of time than GSOs. Why? Satellites sitting in LEO are subject to higher atmospheric drag. The degree to which atmospheric drag affects the lifespan of the satellite depends on where in the LEO the satellite sits (altitude—low (160 KM) to high (2000 KM)) and whether the satellite has station-keeping thrusters (can adjust its orbit over time). For example, depending on the satellite's altitude, atmospheric drag can lead to a fairly rapid decaying orbit or be fairly negligible in a satellite's lifespan. If a satellite is sitting at 500KM or less and dies, it deorbits in less than a decade (single digit years, typically

6 Iridium NEXT operates the largest traditional LEO constellation at 74 satellites.



5 years or less). If you go above 500KM that number increases to a decade and then decades. As a result, satellites in a “low” LEO orbital plane will need some ability to make altitude adjustments, which requires operators to invest more in their systems. As a consequence, pLEO systems are considerably smaller and built to be disposable (often with a design life of about five years).

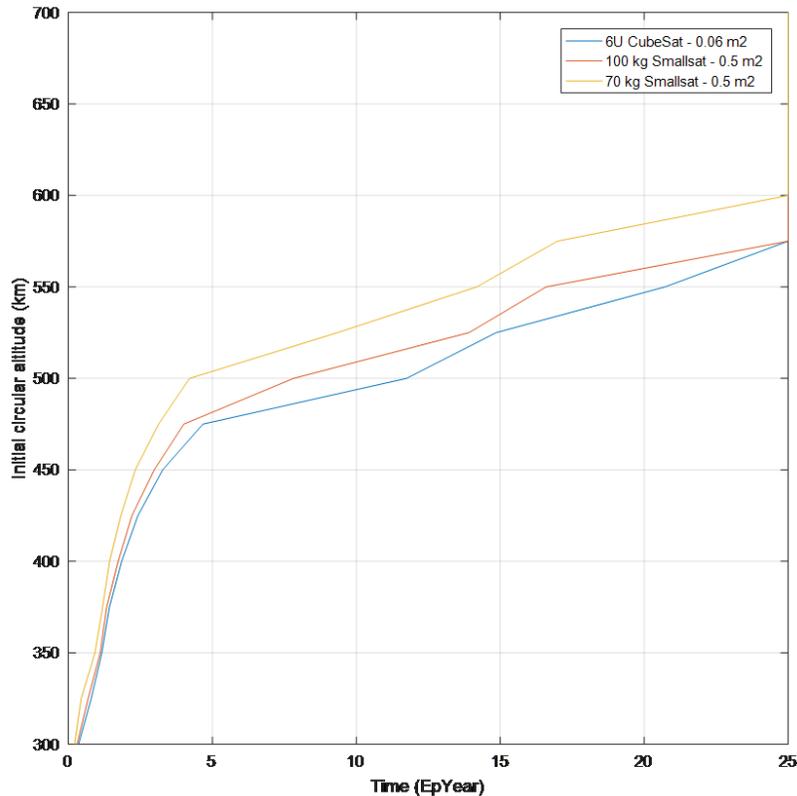


Figure 3. NASA figure showing decaying orbits. Initial orbit altitudes yield different lifetimes depending on the ballistic coefficient of the spacecraft. Three representative area-to-mass ratios are shown. Note that the propagation stops at 25 years, but the initial altitudes yield even longer times. Source: National Aeronautics and Space Administration (2020).

A useful byproduct of a decaying orbit is that it makes it easier to get rid of space junk (satellites that are obsolete or no longer in use). This proves to be a fairly important byproduct when we move from GSOs to pLEOs (swarms rather than smaller satellite constellations). For example, SpaceX deploys (or injects) their satellites in low LEO orbit (around 280KM) before maneuvering them to a higher LEO orbit (about 550KM). This allows them to use atmospheric drag to address any issues that become apparent immediately after deployment (at that altitude without propulsion, the satellite is gone in a few days) and they can deorbit satellites if issues arise later or as a satellite nears the end of its lifecycle (SpaceX expects their satellites to last anywhere between 5-7 years) so that drag works in their favor.

Why didn't we launch swarms of LEOs earlier? The physics of pLEO is favorable for launching many small, relatively disposable systems. Yet, until recently, the necessary combination of launch technology and the electronics, both on the ground and on the satellite, was not affordable or available.



Another significant factor impacting the deployment of LEO systems is the ability of the satellite to “see” the earth. GSO satellites, in a relatively fixed position around the earth, can see roughly a third of the earth and have historically been designed to be in near-constant use, albeit with higher latency. LEO satellites, because of their size, much lower altitude, and constant orbit around the earth, see the earth through a soda straw with a much smaller area of regard on the earth and are designed to broadcast for 15-20 minutes per orbit but with much lower latency, hence the need for swarms. LEOs are smaller than their GSO counterparts, and that smaller size coupled with the reality that launching a satellite into a lower orbit is less costly than launching that same satellite into higher orbit makes them cheaper to lift into space. But the cost savings do not end there. Private operators, namely Blue Origin’s New Shepard and SpaceX’s Falcon 9, have also been able to drive significant launch cost reductions by reusing launch vehicles, which reduces one of the most expensive elements of putting anything into orbit.



Figure 4a. The New Shepard booster lands after Mission NS-15’s successful mission to space. (April 14, 2021). Source: Blue Origin

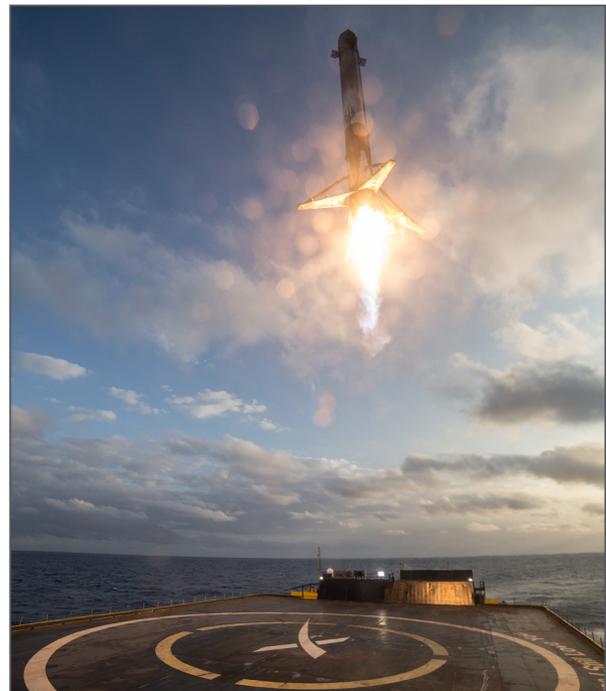


Figure 4b. SES-10 Mission | Falcon 9 First Stage Landing. Source: Official SpaceX Photos (CC BY-NC 2.0)

One important effect of lowering launch costs is that it reduces the pressure on operators to launch as sparingly as possible. Companies such as SpaceX have radically transformed the launch space in general and satellite communications in particular. By way of comparison, AT&T operates a GSO constellation of 14 satellites, each requiring a dedicated launch because each satellite weighs on average 5,600 kilograms with a design life of 15 years (“UCS Satellite Database,” 2021). Contrast this with SpaceX’s Starlink service, which [launches 60 satellites](#) per launch into LEO because each satellite weighs 227 kilograms and is designed for a shorter lifespan (Thompson, 2021). As of [March 2021](#), “SpaceX now has 1,200 Starlink satellites in orbit, having launched 310 of them [in 2021] alone. Five of SpaceX’s seven Falcon 9 missions in 2021 have been dedicated for Starlink, with the other two launching Transporter-1 and the Turksat 5A geostationary communications satellite” (Foust, 2021). Keep in mind that by the time you read this sentence, the number of Starlink satellites in orbit will be even greater.

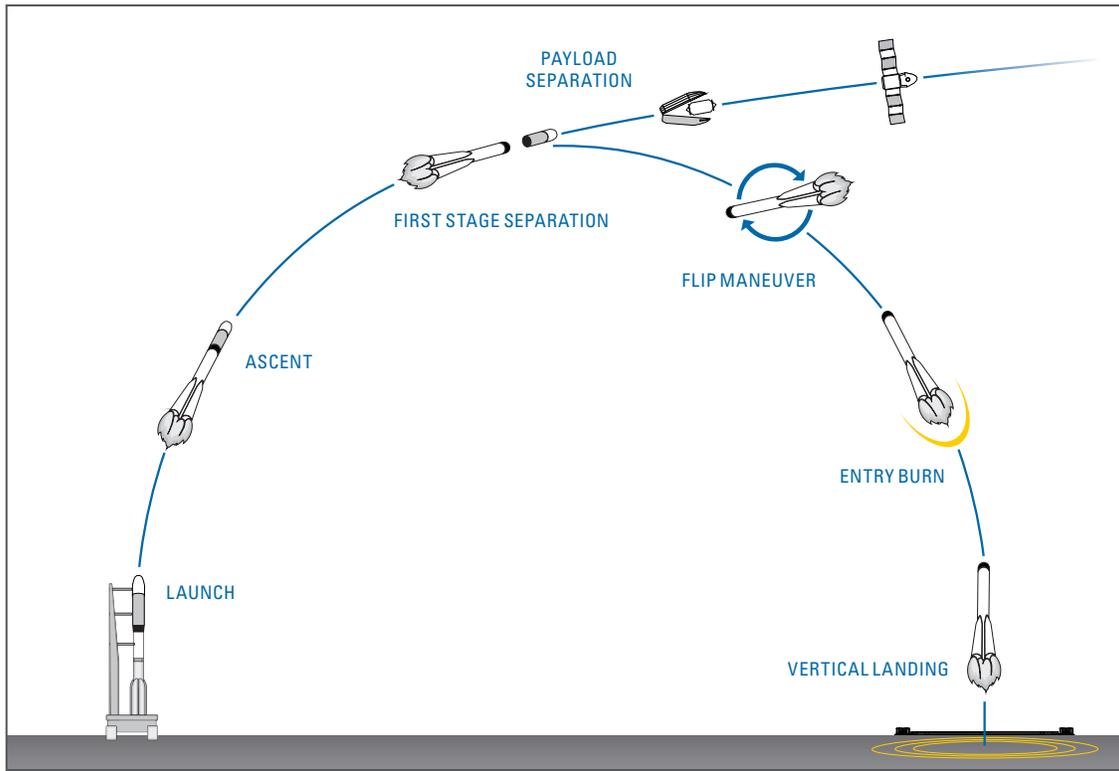


Figure 5. Launch to recovery. Reusable rocket flight scheme.

Notably, not all satellite communication constellation companies have their own launch capabilities. While Amazon’s Kuiper constellations are still being designed, [the company gained U.S. Federal Communications Commission \(FCC\) approval](#) last year (2020) to operate a constellation of approximately 3,200 internet satellites in LEO by July 30, 2029 (Amazon must launch 50% of its constellation by July 30, 2026 to maintain its authorization) (Henry, 2020). To inject those satellites into orbit, Amazon recently [selected United Launch Alliance’s \(ULA\) Atlas V](#) rockets for at least nine of its launches (Sheetz, 2021).

Advancements are not just limited to the launch space, however. Current and legacy advances in electric propulsion systems and microelectronics, such as the development and availability of cost-effective active electronic phased arrays, field programmable gate arrays, and application specific circuits (a type of semiconductor chip or integrated circuit), have accelerated the design and deployment cycles as well as the capabilities of satellites.

Why are pLEOs an advancement? A swarming constellation of pLEOs would provide uninterrupted, real-time, ubiquitous coverage of a region. This in and of itself is a significant shift in how we think about satellite communications. Unlike legacy systems where it was costly and complicated to move data around the earth using GSOs for the “last mile” while still relying heavily on terrestrial fiber, pLEO creates the opportunity to move data around the earth without using terrestrial fiber.

The advancement pLEOs represent is also a story of the business models satellite companies can now pursue. Companies can now approach satellite systems as a service to be sold on to customers rather than a bespoke, sustained business investment that a customer needs to make. For example, [Amazon Web Services \(AWS\)](#)



now offers a “fully managed service that lets you control satellite communications, process data, and scale your operations without having to worry about building or managing your own ground station infrastructure” (Amazon, 2021). In other words, AWS has built a business model around “Ground Station as a Service” that you purchase and then seamlessly integrate into your business operations rather than ground stations as a bespoke investment that you need to invest in and acquire specific equipment to access, tailor to your specific use-case, and then maintain those assets over time. Flexible payloads, such as those developed by [Airbus](#), are another example: offering operators the capability to reprogram satellites’ missions (e.g. reconfigure frequencies, coverages, and/or power allocation) after the spacecraft is in orbit (“Flexible Payloads,” 2021). In short, satellite systems of the past were mission specific and high resource investments. The satellite systems of today, which are currently disrupting that market, strive to be plug-and-play across a wide diversity of telecommunications needs.

What’s the end result? With swarms of LEOs and satellites as a service on the horizon, 5G networks have a viable alternative to fiber for real-time data backhaul. This provides utility for expanding coverage in areas where laying fiber is not economically viable (remote) or feasible (a ship or an airplane). It also provides redundancies and alternatives to backhaul in more urban areas where fiber has already been laid and has the potential to increase connectivity to accommodate an ever-increasing number of connected devices and data traffic (the unique demand an explosion in IoT devices will bring). In short, with the evolution of satellite systems and the requirements of the future 5G proponents promise, 5G will need to rely on an integrated telecommunications system with both terrestrial and space-based components working in tandem.

What Purpose Could Satellites Serve in 5G Networks?

In order to deliver on the full promise of 5G networks (near ubiquitous, instantaneous coverage for a massive number of connected devices), satellites will need to play a far more central role within telecommunications networks going forward, with both terrestrial and space-based components working in tandem for a wider diversity of functions. Given the evolution of the satellite industry, both in terms of business models and technology, that greater role is now, for the first time, possible.

Notably, the specific and diverse roles satellites will play in the future is still an open question and the answer depends as much on industry and business decisions as it does on technological and economic feasibility. However, in 5G networks, satellites could serve three potential functions: providing additional backhaul, creating redundancies, and providing remote and rural areas with greater connectivity. In each of these cases, there is a diversity of business models that could potentially emerge from direct to device connections to connections between the end-user and the core network.

Backhaul: Historically, backhaul (moving data between the radio access network (RAN) and the core network) primarily occurred over fiber or wireless point-to-point. However, increasing demands on telecommunications networks have [increasingly incentivized](#) “mobile network operators around the globe to evaluate different backhaul technologies to meet the rapidly increasing demand for their 4G/LTE network deployments” (“iDirect SatHaul-XE™ Overview”). The need for a greater diversity of backhaul options will only increase as 5G deployments progress. Why? As the number of small cells (low-power, short-range base stations (wireless transmission systems) covering limited geographic areas) in the radio access network (RAN) increases, so too



does the demands on backhaul between the RAN and the core network. Now, with swarms of LEOs on the horizon, 5G networks have a viable alternative for real-time data backhaul (Mosher, 2016).⁷ Given the demands on 5G networks and the evolution of satellite systems, it is possible for satellites to complement existing backhaul mechanisms to meet the growing demand.

Redundancy: In addition to increased demands on backhaul, with the move toward pLEOs, satellites now have the potential to provide overlay networks duplicating segments of the terrestrial networks. This overlay network could replace or augment existing terrestrial networks if those networks experience reduced functionality due to man-made (physical or cyberattacks but also simply mistakes/accidents) and natural disasters. While their utility

...the promise of satellite systems for 5G networks rests on their ability to help us increase the scale and scope of access to these networks; meet increasing demands on these networks, especially in rural and remote areas; and incorporate redundancy in critical segments of these networks.

would be limited, they could potentially prioritize critical services and buy operators time to restore access to terrestrial networks. In short, given that 5G networks will be essential for the daily functioning of not only our economy but society, government, and military, they represent a potential single and catastrophic point of failure. Satellite systems overlaying aspects of terrestrial systems deemed strategically important or essential for emergency operations in the event of a catastrophe can provide those systems with additional resiliency through redundancy.

Remote and Rural Connectivity: Historically, GSOs have been critical for solving the “last mile” problem. With the proliferation of swarms of LEOs, that role could increase both in terms of scale (number of connections) and scope (where those connections can be made). 5G networks will bring with them an exponentially growing number of connected devices, including mobile phones but

also a vast array of IoT devices including billions of sensors. Think rural hospitals carrying out remote surgeries; cars traversing interstates, planes in flight, and ships out at sea; and agriculture fields full of sensors. While their utility in dense urban areas is more limited (satellites require line of sight for a direct connection to a device), the opportunity now for Massive Machine Type Communications (MMTC) and the fact that many of these devices will be scattered over wide geographic areas increases demands on data collection and distribution across 5G networks. Here too, satellites, integrated into terrestrial telecommunications networks through new network architectures, can provide an important solution by leveraging the wide satellite coverage enabled by pLEOs. In this regard, one of the biggest benefits is that LEOs, unlike GSOs, can now deliver a real interactive experience, a degree of connectivity often lacking in rural and remote areas to date. With the addition of more fully integrated satellite systems into 5G networks, connectivity can be expanded to remote areas where laying fiber is not economically viable (communities across the United States and around the world) or feasible (an oil rig off the coast, a ship traversing the ocean, or an airplane flying overhead).

⁷ For example, SpaceX has openly acknowledged that each of its satellites has approximately 20 Gbps capacity with a recent [SpaceX FCC filing](#) indicating that “[each] satellite in the SpaceX System provides aggregate downlink capacity to users ranging from 17 to 23 Gbps, depending on the gain of the user terminal involved.”

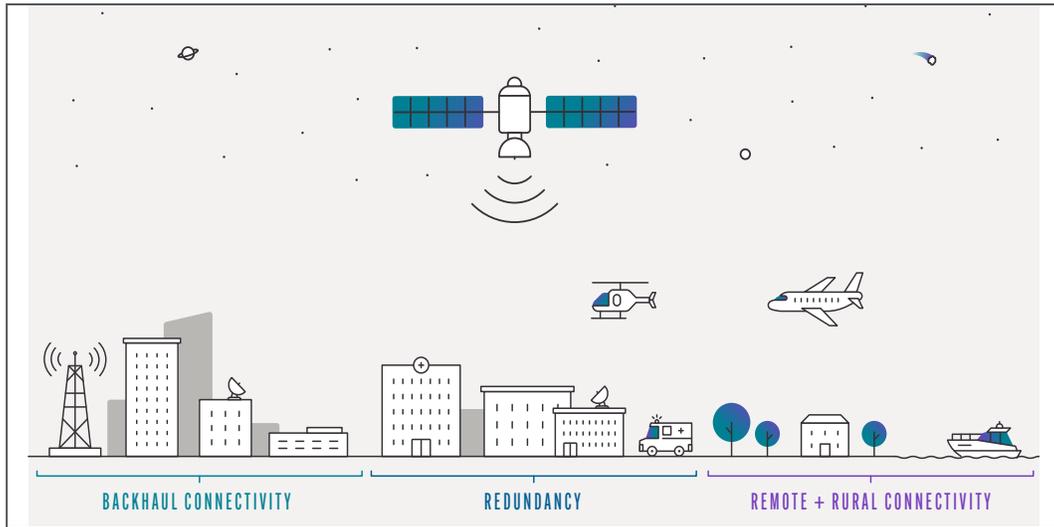


Figure 6. Three Potential Uses for Satellites in 5G networks.

In conclusion, the promise of satellite systems for 5G networks rests on their ability to help us increase the scale and scope of access to these networks; meet increasing demands on these networks, especially in rural and remote areas; and incorporate redundancy in critical segments of these networks. Evolutions in underpinning technology and the diversity of business models companies can now pursue makes this integration not only possible but feasible. Though this outcome is far from certain and would require investment in and a willingness by both the satellite and 5G communities, this goal has increasingly become a sustained focus of the technical standards bodies, researchers, and industry in an effort to make the 5G promise a local and global reality.

Satellites, the (Not So) Novel Critical Infrastructure Problem

Given the [economic, social, and strategic importance of 5G networks](#), 5G represents the latest iteration of critical infrastructure protection challenges (Griffith, 2021a). Satellite systems, their architectures and business models, are increasing and will need to be further integrated with terrestrial telecommunications networks, a move that would not have been possible for prior generations of mobile networks and communications more broadly (due in part to the higher latency associated with GSO). As a result, when we focus on the challenges of maintaining secure, resilient, and defensible 5G networks, we must broaden our focus from the traditional terrestrial aspects of these networks to include space.

In short, 5G and ubiquitous space-based networks increases an already vast threat surface. Concerningly, the security, resilience, and defensibility of space-based systems has long been overlooked in favor of survivability of these systems given the rigors of space.

However, in seeking to address this gap, space is all too often presented as entirely novel, an area where all prior lessons fall away and completely new issues arise. In many instances, such as radiation hardening, thermal management, or power management, this is true. The rigors and inaccessibility of space do create challenges for maintenance and durability unlike almost anywhere else we operate. In addition, the geopolitics of space—a



domain simultaneously dominated by intense competition, deep cooperation, and vast economic impacts—brings with it its own unique challenges. However, when it comes to questions of national security related to space’s role within critical infrastructure and services, many of the same concerns that emerge when focused on the earth still apply when looking to the stars.

Those (not at all novel) concerns fall into two broad buckets: (1) defending the systems themselves and (2) ensuring the security of the data traversing these systems. In practice, a malicious actor could deny the United States access to components of its 5G networks by targeting the physical and digital architectures that underpin that system. This type of malicious operation seeks to prevent the United States from using these systems for their intended purpose. A malicious actor could also inflict harm by gaining access to the information passing through, stored on, or generated by 5G networks (from personal phone calls to intellectual property revealed on factory floors and agriculture yields recorded by sensors deployed in field to troop movements around the world). This type of malicious operation attacks network users’ ability to use their data with confidence, or at all. Despite the novelty or uniqueness of the communications path or waveform, the core challenges to confidentiality, availability, and integrity are still present in satellite communication systems.

...when it comes to questions of national security related to space’s role within critical infrastructure and services, many of the same concerns that emerge when focused on the earth still apply when looking to the stars.

In its simplest form, critical infrastructure protection—its security, resilience, and defensibility—is a risk management problem.

Mitigating risks requires first identifying (a) potential failure states for a system and then (b) how to avoid some of those failure states, maintain critical functionality in the event of others, and restore functionality in the wake of those that take a system down. In plain English: what requirement is the operator designing to (what do they think the threat is), how does the operator plan to protect its networks, and what backups and mitigations are in place if that protection fails?

In practice, these efforts boil down to three categories of concern: (i) the physical infrastructure or architecture (physical security), (ii) the digital systems operating on and the data traversing that infrastructure (cybersecurity), and (iii) the supply chains (both hardware and software) that comprise these systems (supply chain security). However, there is also a first-order question that precedes these three concerns: (iv) the criticality of the use-cases these networks support. This criticality question is the metric by which we determine what counts as critical infrastructure and services. It is also the means by which we assess the costs we are willing to incur in order to increase security, resilience, and the defensibility of these systems across the three metrics listed above.

Notably, taken together, these four concerns (criticality, physical architecture, data and digital systems, and supply chains) mirror the categories of concern that arise with critical infrastructure more broadly, including our current 4G LTE networks and sectors outside of telecommunications such as energy, water, food, healthcare, and transportation. Despite the remoteness of space, when it comes to assessing the degree of and categories for concern, satellites are a not-so-novel critical infrastructure problem. Moreover, and worth mentioning here, the addition of satellite systems to terrestrial 5G networks also presents another potential path to create resiliency and possibly move around compromises in confidentiality, availability, and integrity within 5G networks more broadly.



Before delving into the ‘four questions to ask regarding national security concerns associated with satellite systems in 5G networks’ in the next section, we need to lay out a few scope conditions for this paper. It is important to note that, for malicious activity targeting critical infrastructure and services, there is a graduated scale of escalation. [While telecommunications infrastructure can, has, and will be targeted during periods of armed conflict or warfare using kinetic means \(satellite systems will likely be no exception\),⁸](#) these instances are not the focus of this paper (Harrison, Johnson, & Young, 2021). Such kinetic operations by an adversary require a very different defense and national security discussion than the one offered here: one with limited security and defensibility solutions but high redundancy and resiliency requirements as well as the contingency planning necessary to carry out warfighting without access to telecommunications networks. Here we focus our and your attention on the potential national security risks associated with reliance on satellite segments by 5G telecommunications networks short of a physical assault on critical infrastructure for tactical and operational purposes.

Worried? Four Questions to Ask

For policymakers, and government officials, interested in addressing national security concerns associated with satellite systems within 5G networks (or any telecommunications networks comprised of terrestrial and space-based architectures), the following are four questions to (a) help you assess the current security, resilience, and defensibility of satellite systems in general in addition to a specific satellite system in particular⁹ and to (b) keep in mind when considering how the government - in cooperation with the companies developing, deploying, and operating 5G satellite systems and the users of these systems - can increase the security, resilience, and defensibility of these systems going forward.

Q1 Criticality:

Who depends on a particular satellite system (now and in the future), to what degree, and for what purposes?

Q2 Physical Architecture:

What does the ground teleport infrastructure and launch capabilities look like, and where are they located?

Q3 Data and Digital Systems:

How does the system protect the data it is moving and ensure that the data keeps moving reliably?

Q4 Supply Chains:

Which, and how many, vendors comprise the satellite system’s (hardware and software) supply chain?

Under each question we have provided a series of probing questions that help shed light on the larger, parent category. These probing questions are not meant to be an exhaustive list, but rather an informative one. As the technologies underpinning satellite systems, as well as the tools, techniques, and procedures (TTPs) and goals of malicious actors evolve, so too may the list of relevant probing questions. These four overarching questions, however, will endure.

⁸ Blowing up a ground station or deploying anti-satellite weapons designed to incapacitate or destroy satellites, for example.

⁹ Importantly, you cannot judge the overall security, resilience, or defensibility of satellite systems by solely examining the few well known players dominating headlines.



These probing questions, like their four parent categories, are focused primarily on (1) framing the scale and scope of the national security concerns that emerge from the expanding threat surface as the role of satellites in telecommunication networks (i.e. 5G) evolves and (2) providing insights into and opportunities for policy engagement with industry to assess not only the state of play but to develop and pursue informed policies going forward.

As a result, we have discarded important security questions relevant for systems' operators in favor of probing questions that help inform actionable government policies and initiatives. For example, a cybersecurity professional tasked with the security of these satellite systems would need to know if they were using a transponded or processed system. This distinction is critical because of the nature of space-based communications. Depending on the satellite architecture, the satellite may just relay a data stream (this is known as a transponded, or "bent pipe," system). Alternatively, the satellite's communications waveform or modes may require the data to be processed on board the satellite, which means that the satellite's onboard systems may have direct access to the data being transmitted (this is known as a processed system). The increased access to data being transmitted associated with processed systems raises additional sets of cybersecurity concerns that a satellite system provider should be prepared to address. However, while this is an important distinction for the operator of or security professional focused on the satellite system to be aware of, it is not a distinction that is most directly relevant to or actionable by the broader national security minded policy community.

Finally, though the focus of this brief is on satellite systems relevant to 5G networks, these four questions and many of their probing questions can and should be asked of any satellite system more broadly. Additionally, many of these questions also provide important leverage for telecommunication providers and other users of communication satellite systems given that the security and resilience of these systems is also an important business consideration (though at a different scale and scope than the national security concerns highlighted explicitly here). Therefore, while this paper is focused primarily on the national security concerns driving critical infrastructure protection for 5G networks, many of the lessons outlined here have far wider utility.

Q1—Criticality: Who Depends on a Particular Satellite System (Now and in the Future), to What Degree, and for What Purposes?

Assessing and managing national security risks is, at its core, the same calculation undertaken when assessing and managing risk more broadly: assessing the likelihood and the potential consequences of an event relative to the costs incurred in order to prevent it or mitigate its impact. When we narrow our focus to the role of satellite systems in 5G networks, this raises the question of what we use these networks for: what data traverses these systems and what other critical infrastructure and services rely on them for their daily functioning. In other words, the United States' level of dependence on 5G networks more broadly, and the role of satellites within those networks more narrowly, determines whether these systems rise to the level of national security concern in the first place and to what degree.

Questions of criticality are not merely theoretical or academic in nature. In the last 30 years, broad targeting of commercial communications infrastructure is standard behavior for state-backed intelligence agencies. It is



reasonable to assume that the new satellite constellations will be subject to this same behavior. This shifts the criticality of commercial systems and creates the need for a more deliberate consideration of what risks they are carrying. It also puts satellite operators, like other private operators of critical infrastructure, in a unique situation: where their security, resilience, and defensibility efforts are not merely of commercial import for a company, but of national import for a state.

Asking this question first, therefore, allows you to gauge the necessary degree of security, resilience, and defensibility of various satellite systems within the broader 5G ecosystem. Not all systems are equally critical and therefore worth the same degree of investment.¹⁰ Remember, security, resilience, and defensibility are not cost-less considerations. Systems designed for national security purposes and moving national security data, for example, merit far more stringent security practices than systems moving general commercial data. Additionally, systems serving a redundancy function for emergency services merit far more stringent security measures than

...security, resilience, and defensibility efforts are not merely of commercial import for a company, but of national import for a state.

satellite backhaul for nonessential services, just as a system that is the sole source of connectivity in a critical area rather than one of many servicing that area do.

In other words, the answer to ‘how worried you should be and therefore how much you should invest in the security, resilience, and defensibility of these systems’ is dependent on the position of specific satellite systems within the broader 5G architecture.

Yet, unlike the following three questions, this is also a question that the satellite provider will be least equipped to judge. A satellite provider, for example, should not have significant insight into the data actively transiting their networks (such visibility would raise its own sets of privacy and security concerns). Instead, this question relies on users of those systems to assess their security needs. It also requires the policy community to step in and make robust local, regional, and national risk landscape maps and assessments that then shape the policy decisions they enact for operators, vendors, and customers in a given area serving a specific function. As such, this question persists as one the most challenging national security questions to answer for any segment of critical infrastructure because it requires significant (a) visibility into our own complex national risk landscape, much of which lies in the private sector and where each actor only has visibility into their own unique segment, and (b) the development of policies for risk reduction and management for the critical dependencies identified in that process.

Probing Questions:

1. What data traverses which networks?

Here the concern is how appealing a target the data traversing those systems is likely to be. Communications networks (digital or otherwise) have long been the [target of intelligence operations](#) by state and non-state actors alike (Buchanan, 2020). [5G will be no different](#) (Griffith, 2021a). Within that breadth, you are looking to identify data that malicious actors, such as strategic rivals, would greatly benefit from gaining access to or denying

¹⁰ Note: investment here does not imply that a satellite operator should bear the entirety of the costs associated with building out their systems to account for national security concerns by persistent and/or dedicated adversaries. Investment is used generally here to connote the joint industry and government lines of effort.



someone else access to. Then, given that information, determining where certain types of data should flow given the security structures in place or how to harden systems where those data flows are likely to occur. For example, the defense industrial base relies on these types of networks for their daily operations as do militaries for command and control (C2) over troops in the field.

However, it is important to remember, not all information passing through a network rises to the level of national security concern. Most of the data traversing commercial 5G networks isn't national security data. However, while there is a critical difference between specific types of data (e.g. troop movements versus my personal phone call to a family member, versus point of sale financial data), data other than national security data can also create a national security risk. Indeed, [cyber espionage operations that gather data in aggregate can also have significant national security consequences](#) both in terms of laying bare national vulnerabilities but also facilitating intellectual property theft (Griffith, 2021b). In short, national security data, intellectual property (IP), and data in aggregate can prove to be appealing targets for malicious cyber actors.

Recall, however, a commercial satellite operator selling satellites as a service for 5G networks may not, and very likely does not, know the specific character of the data traversing their systems without having a very specific and detailed conversation with their customers. This visibility is available only to the user (whether that be specific national security industries, the government, or the military). In some cases, users—namely, the U.S. government—have implemented data-specific standards based on the criticality of the data traversing a network (i.e. the [Committee on National Security Systems' \(CNSS\)](#) information assurance standards for commercial satellites that carry classified or otherwise sensitive data). Yet, none of these efforts focus on the risks associated with data in aggregate, something 5G networks will have in spades. Importantly, this question is as applicable to 5G and pLEO satellite communications as it is legacy communications systems; the density of data increases the risk we are confronted with as we adopt new technology.

2. *What services and/or infrastructure do they support?*

This question focuses on the position of satellites within the larger daily functioning of the government, military, society, and economy. Within the United States, this critical infrastructure conversation has largely been the responsibility of the Cybersecurity and Infrastructure Security Agency (CISA) under the Department of Homeland Security (DHS) and relevant sector-specific agencies¹¹ in cooperation with sector-based organizations such as Information Sharing and Analysis Centers (ISACs), private security companies such as Dragos and FireEye, and the critical infrastructure and service operators themselves. Though, even in these bodies, the focus has largely been on information sharing, security best practices, risk mitigation strategies, and incident response rather than comprehensive threat landscape mapping.

This line of inquiry, in particular, focuses our attention on building out robust risk landscape models. These can and should occur at multiple levels: e.g. the level of particular telecommunications operators (their networks), the customer (their use-cases), and local and national jurisdictions (the national, regional, state, or city landscape). The question here is not one of 'importance to' but rather 'essential to' their functioning. Moreover, dependency is not

¹¹ For example, DHS is the designated sector-specific agency for communications while the Department of Treasury is the designated sector-specific agency for financial services.



just about who relies on them, but also how much they rely on them. What role do they play? Redundancy? The last mile? Backhaul? Does national defense—military or intelligence—rely on their networks for mission critical systems? The answers to these questions indicate the criticality of the system. The higher the criticality, the greater the need for security, resilience, and defensibility of that satellite system.

Here too, however, the satellite provider, especially those selling satellite coverage onto users as a service, does not have the best visibility into these questions. These sets of probing questions can be best answered and addressed by leveraging information held by the government (local, state, and national), organizations such as ISACs (e.g. the [Communications](#) and [Space ISACs](#)), and customers of these services (whether that be a telecom operator, a factory, or the U.S. military) (“National Coordinating Center for Communications”).

O2–Physical Architecture: What Does the Ground Teleport Infrastructure and Launch Capabilities Look Like, and Where are They Located?

This question focuses on the survivability and dependability of the transfer between space and ground assets. Getting data into space is only part of the solution; moving that data back down to end-users makes the system effective. [A poorly designed or insecure ground infrastructure is an easier target than the space-based assets themselves](#) (Gibson, 2018, and Informa, PLC). Yet, a dispersed system with redundancies is more difficult to cripple than a system with clear chokepoints, such as a limited number of uplinks/downlinks. Finally, as previously discussed in the prior criticality section, the locations of these ground sites should also be evaluated depending on the use-cases they support.

A poorly designed or insecure ground infrastructure is an easier target than the space-based assets themselves.

The following probing questions focus on security and resilience, but they approach those concerns from different vantages within the communications satellite ecosystem. All four probing questions hinge around two lines of inquiry: (1) do satellite providers understand the potential failure modes (one measure needed to assess risk) for their systems and (2) how have they sought to mitigate or address those failure modes in practice.

Probing Questions:

1. *How many connections to the ground, uplinks and downlinks, do they have per satellite?*

This question focuses our attention on increasing resilience through redundancy for one important segment of the satellite system. As previously mentioned, satellite systems function for terrestrial purposes only when they can get data up and down from space. As a consequence, the link segment provides another opportunity for insecurity and failure. The goal here is to ensure resilience in the event that an uplink or downlink fails. In other words, how many failures of various types can they sustain before they lose access to their constellations? As a general rule of thumb, you hope to see them implementing the ‘rule of three’¹² whenever possible and especially in mission critical components of their network such as uplinks and downlinks.

¹² The “rule of three” is a network engineering rule of thumb asserting that creating resiliency in a critical network node takes at least three diverse physical links to that critical point in the network.



2. *Are their ground teleport sites dispersed across a geographic region or are they clustered? And if they are clustered, how do they manage the physical and digital security given that location?*

This question also focuses on resiliency, but now with a focus on upstream dependencies and potential points of failure. For example, asking this question will help you assess concerns over physical risks to their ground-based assets. Having ground teleport sites dispersed across a geographic region rather than clustered provides greater resiliency within the system to weather (heavy rain and wind for example) as well as to natural disasters and physical attacks. Put more simply, a natural disaster in one area resulting in a loss of access to the majority of

This line of questioning raises an important question for the U.S. government: namely, under what conditions should we consider commercial base-stations strategic assets?

or all their ground stations would be deeply concerning. Notably, clustered ground teleports may also rely on the same physical or digital infrastructure to operate, electricity grids for example, which are subject to their own critical infrastructure, national security, and cybersecurity concerns.

If their ground stations are clustered, the follow-up question is how they mitigate the risks associated with clustering their ground teleport sites. This line of questioning focuses on the degree to which they have put measures in place to mitigate the risks associated with their specific teleport locations and if those

measures are sufficient given the role their satellite networks play in the larger 5G architecture. Answers here should include contingency plans in case of emergency, such as an alternative power source in the event of a grid failure. However, they should also address concerns over physical security that might arise if those sites are located in countries or localities with tenuous relations with the United States or that have demonstrated an inability to maintain a monopoly on violence within those areas. Access questions might also arise if teleport sites are clustered in countries located in geopolitically contentious regions where conflict might erupt in the future (this has been a concern, for example, around Taiwan's pivotal role in the semiconductor supply chain given its proximity to China and China's historical claim over Taiwan). Finally, given geopolitical tensions, access to ground stations can also be leveraged as a tool of statecraft. Take, for example, [the 2003 incident between China and the small Pacific state of Kiribati](#) (Jones, 2016). China shut down its control station in Kiribati after Kiribati established diplomatic relations with Taiwan. China later [restored diplomatic ties](#) with Kiribati in 2019, but the incident shines a bright light on the ways in which ground control of space-based assets can be politicized (Crossely, Jones, & Blanchard, 2020). This line of questioning raises an important question for the U.S. government: namely, under what conditions should we consider commercial base-stations strategic assets?

In sum, in the satellite providers' answers to this line of inquiry you want to see (1) an understanding of their risk landscape based on location and (2) plans in place to mitigate those risks in practice across a variety of potential failure modes (e.g. weather, power outage, natural disaster, physical attack). While you will need to then assess whether the risks have adequately been taken into account given the use-cases they support or whether their risk management strategies are sufficient, this probing question provides an opening into that broader, detailed discussion for individual providers but also across the industry as a whole.



3. *How do they evaluate the risk to the information traversing their network based on the ground teleport sites?*

While the former line of questioning focused on losing access to physical architecture, this question addresses concerns of information security stemming from undue physical access to satellite systems. In this specific case, the location of ground-based assets. In addition to concerns around cyber espionage operations targeting the data traversing communications satellite systems, the location of the teleport sites can provide opportunities for physical (human) access to that data. For example, insider threats: an employee abuses their privileges to compromise the systems and/or the data traversing those systems. Another example, however, can emerge from easy, or rather easier, access, to the physical sites themselves by local actors. Like the question above, satellite providers' answers help assess the degree to which they understand their risk landscape and have put measures in place to mitigate the risks associated with their specific teleport locations.

4. *Is the satellite built like a capital investment (i.e. an aircraft carrier, designed for a 50 year lifespan) or is it built like your cell phone (i.e. designed for a 2 year lifespan)?*

This fourth, and final, probing question focuses on maintenance of systems and how a lack of physical access over longer lifetimes increases the necessary, upfront security and resiliency investments. Notably, this question also straddles physical security concerns (Q2) and cybersecurity concerns (Q3).

One of the primary security concerns associated with legacy satellite systems (GEO/GSOs) is that they average 15 years of use.¹³ This reality was due, in large part, to limitations around launch but also the costs of design for each satellite. Because of the cost of design and launch, legacy satellites were built for long term survivability and reliability (primarily assessed by their ability to carry out their payload, which given the lifespan and the cost would hopefully be a diverse set of functions). Upgrades, sometimes software but often hardware, required direct human intervention. The pLEO constellations, however, are built for specific purposes with planned obsolescence in mind. As a result, it is more cost effective to launch new satellites than it is, in some cases, to modify the existing satellites. Moreover, at the planned altitudes for some pLEO constellations, atmospheric drag will eventually de-orbit the satellites without altitude adjustment (they fall out of the sky and, therefore, need to be replaced more frequently).

As a general rule of thumb: the higher the cost to upgrade, the higher the bar should be for initial security and resilience measures.

Since a diversity of satellite constellations will play a role in future telecommunications networks, this question helps assess the space-based assets deployed and utilized by a specific operator and the lifecycle of and costs for maintaining those assets over time. As a general rule of thumb: the higher the cost to upgrade, the higher the bar should be for initial security and resilience measures. Take for example, the Hubble space telescope. Maintenance over its lifetime has required four service missions, the earliest of which was three years after its launch in 1990. Luckily, as [NASA has noted](#), "Hubble was the first telescope designed to be visited in space by astronauts to perform repairs, replace parts, and update its technology with new instruments" ("About – Hubble Servicing

¹³ The 66 satellites in the Iridium Constellation were launched between 1997 and 2002, the Eutelsat constellation of 39 satellites has been launching since 2000, and their oldest satellites are still operational.



Mission,” 2021). As another example, outside of the software development and test process NASA uses, [the agency spends an additional 10-20% of their software budget](#) conducting independent verification and validation of software to ensure that software works as designed (Hunt, 2012). Why? Discovering vulnerabilities, mistakes, and/or unexpected failure states post-launch where access is deeply constrained would be deeply costly and difficult to address at best and catastrophic at worst. This is especially true in the case of human space flight.

In short, when a satellite is built like a capital investment (e.g. an aircraft carrier), those assets require modernization and maintenance over their lifetimes to remain reliable, functioning, and secure. In space, modernization and maintenance, specifically of physical components (if your architecture does not accommodate securely pushing code up to your main system bus and payloads, you have a major problem in your design), is very costly. This places a far higher burden on initial security and resilience designs for those systems.

In contrast, systems with shorter lifespans (e.g. a LEO satellite) and/or easy physical access (e.g. a mobile phone), face a different set of tradeoffs. SpaceX satellites, for example, require good engineering but not exquisite resilience and security because they have shorter lifespans and can be more readily replaced by launching new ones if the need arises. The same cannot be said for a GSO satellite, which has a far longer lifespan and costs far more to put in orbit.

Q3 - Data and Digital Systems: How does the System Protect the Data it is Moving and Ensure that the Data Keeps Moving Reliably?

This third area of concern focuses on the confidentiality, integrity, and availability of data traversing the system and the data used to operate, monitor, and secure that system. Satellite systems, like critical infrastructure more broadly, utilize both information technology (IT) and operational technology (OT) fusing the digital and

...not only are these satellite systems vulnerable to hacking, but we have a poor cybersecurity track record with commercial satellite systems to date and the number of actors capable and keen to target these systems is only likely to increase.

physical worlds. A poorly designed digital ecosystem can be just as damaging (if not more so) to national security as a poorly designed physical architecture (the prior question) – both in terms of the opportunities for destruction and disruption of services but also opportunities for intelligence gathering by malicious actors.

Data security, or cybersecurity, is a pressing policy challenge now and it is also only likely to become even more pressing in the future. As Meg King and Sophie Goguichvili, Director of and Program Assistant with the Woodrow Wilson Center’s Science and Technology Innovation Program (STIP) respectively, have [pointed out](#), “in the near-term, these kinds of [cybersecurity threats] will likely remain posed by nation state actors but as more communications capabilities come online via space, the group of actors could expand to well-resourced non-state actors (e.g. criminal groups) seeking financial gain” (2020). In short, not only are these satellite systems vulnerable to hacking, but we have a poor cybersecurity track record with commercial satellite systems to-date and the number of actors capable and keen to target these systems is only likely to increase.



Probing Question:

1. *Do satellite providers understand their attack surface and failure states, and do they implement defense-in-depth to address both?*

This questions assesses (1) whether the system provider understands their own attack-surface (their systems, including everything operating on, connected to, and interacting with those systems), (2) what system failure states are possible given that terrain, and (3) if they have developed and actively deploy defense-in depth to address concerns with both 1 and 2. Defenders get to pick the terrain upon which malicious operators engage (their space-based systems and supporting ground communication systems). As such, they should understand the terrain they have built for themselves and they can, and should, build and maintain that terrain to their advantage. Defense-in-depth, an approach developed by and well documented within the broader cybersecurity community, requires an understanding of that terrain - coding conventions, number and type of connected devices, software and hardware inventories, etc. - in order to employ a diversity of measures to hamper malicious actors' efforts to gain access to, maintain access in, and take action on (exfiltrate, alter, or deny access to data) their systems. Concerningly, however, defense-in-depth has historically been largely overlooked when it comes to the cybersecurity of satellite systems.

Defense-in-depth requires a wide range of [computer network defense](#) investments spanning four broad categories: (1) architecture (e.g. network segmentation, limitation of privileges, network protocols, logging/record keeping of activity, etc.), (2) passive defense (efforts that require limited human oversight, such as automated network monitoring, e.g. firewalls or virus scanning software), (3) active defense (network monitoring that requires active human participation, such as red teaming, analysts, and bug bounties), and (4) intelligence gathering (focused on discovering, analyzing, and providing actionable information on vulnerabilities in their own system, malicious activity in their own networks, and malicious activity targeting systems not, but similar to, their own) (Lee, 2015). For example, if they are using open-source software within any segment of their satellite system, what standard operating procedures have they put in place to ensure the security of that software when it is first acquired and deployed in their system, to actively monitor that software for vulnerabilities (utilizing both static and dynamic testing tools), to address vulnerabilities and areas of concern before they are exploited, and effectively respond and recover if malicious activity is discovered. If they are using proprietary software developed for their specific system, the same questions apply.

Defenders get to pick the terrain upon which malicious operators engage. As such, they should understand the terrain they have built for themselves and they can, and should, build and maintain that terrain to their advantage.

It is important to note, defense-in-depth requires dynamic assessments of potential failure modes (stress testing systems and yes, sometimes, breaking assets) in order to fix vulnerabilities but also to develop the ability to recover in the event of crisis. Without this knowledge, incident response in real time will be severely and potentially catastrophically hampered. Perimeter defense, denying malicious actors access to your network, has long been recognized as insufficient for ground based IT systems. That same reality should be, though is [often not](#), reflected in satellite IT systems (Bailey et al., 2019).



Moreover, cybersecurity should be a central consideration as early as the research and development (R&D) stages and not an add-on product integrated into a system as an afterthought. Systems should be designed and maintained with both the security and resilience of that system, as well as the defensibility of that system, in mind. Yet, this is often not the case given the costs associated with baking in cybersecurity from the start and the less visible outcomes that investment produces when compared to other investments a company could make. For example, if an engineer faces a decision to either invest funds in running an additional assessment of how robust their satellite's payload is to the rigors of space versus investing those funds and time into a cybersecurity

...cybersecurity should be a central consideration as early as the research and development (R&D) stages and not an add-on product integrated into a system as an afterthought.

risk assessment of that system, from a business perspective, the former provides more tangible benefits while the latter often feels more abstract.

Given that business incentives can lead to an under prioritization of cybersecurity and that cybersecurity is a complex task that must evolve over time as systems, malicious actors, and our baseline knowledge evolves, government can play an important role in both assessing the state of play across the industry, but also in identifying persisting gaps and where further support and clarification is needed.

While some cybersecurity standards for commercial satellites, which include communications satellites, exist (namely the previously mentioned [CNSS'](#) (2016) information assurance standards for commercial satellites that carry classified or otherwise sensitive data), few broader regulations, and even fewer that take into account the diversity of cybersecurity concerns outlined here, exist in this space. Asking satellite system providers this particular probing question serves as an important step in building out those standards and accompanying regulatory frameworks, especially given how important industry led and informed solutions will be going forward, as [King and Goguichvili have previously illustrated](#) (2020).

As such, this line of questioning serves two purposes: (1) to assess the state of play in general but also in relation to a particular provider and (2) to utilize that state of play, including best practices and persisting limitations, to inform better government cybersecurity policy for telecommunication satellite providers today and in the future.

2. *How do they secure data from inject to exit of their infrastructure? And what do their shared responsibility models look like?*

The focus here is on the data flowing through the system. This includes a wide variety of security best practices—encryption, session security, security protocols, active and passive monitoring, intelligence gathering, etc.—that all seek to increase the security of the data traversing networks. This line of inquiry could include specifically asking whether the satellite system uses standard protocols (like IPV4 or IPV6) along with session-based security like Transport Layer Security (TLS). And then, if they instead use a property standard, how have they documented, published, and evaluated that standard.

Another question to ask here is whether the satellite system provider enables customers to bring their own encryption/security solutions. This customization option would allow certain customers to increase the security of their own data depending on the sensitivity of that data. It also raises, however, questions over who is



responsible for securing that customer's data as it traverses the satellite network: the customer or the satellite system provider. How much risk is the provider willing and/or required to take on the customer's behalf? Should we view pLEO carriers as analogous to the Verizons, AT&Ts, and CenturyLinks of the world—as ISP providers or mobile service providers that move data, while the responsibility to secure that data lies primarily at the level of the customer? Or should we view satellite constellation providers as we view major cloud service providers who transport, process, and store customer data, where the responsibility to secure that data lies primarily with the cloud service provider?

There are a handful of potential options for shared responsibility models for 5G satellite providers, each with their own strengths and limitations. However, in the end, there does need to be an answer on where responsibility lies in this ecosystem.

3. *How has end-point security been addressed?*

One final data security concern relates to the handoffs between terrestrial 5G network functions and the satellite ground and space-based infrastructure. Remember, satellite systems in the context of 5G are not standalone networks, but rather integrated within a broader telecommunications ecosystem. This means that a satellite system's operator is receiving data from one segment of that network before handing that data off to another segment. Both the inject and exit points (network end-points) are outside the satellite system operator's control and visibility. All of these endpoints, however, are part of the satellite system's attack-surface (i.e. terrain that must be defended) and provide malicious actors with opportunities to hack these systems.

Therefore, it is critical for a satellite provider to, first, know about and, second, secure all end-points. This process becomes even more important in deeply interconnected ecosystems or webs. As a result, in the case of 5G networks, the concern is even more heightened.

Here, IoT devices will be increasingly and directly leveraging satellite systems. Each new device increases the attack-surface and entry points. Additionally, these devices bring with them software and hardware vulnerabilities of their own, and [security is not a word that gets associated with IoT](#) (Griffith, 2019).

This puts the question of IoT security front and center both for communication satellite providers but also for policymakers tasked with addressing this persisting and ever-growing area of national security concern. It also requires, however, satellite providers (like other providers operating within deeply interconnected ecosystems) to secure handoffs between terrestrial 5G network functions and the satellite ground and space-based infrastructure. One potential path forward here is to require that satellite systems and security architecture leverage a [“least trust” model](#) for system security (“Embracing a Zero Trust Security Model,” 2021). A “zero trust” or “least trust” architecture operates under the assumption that no user, device, application, or service should be universally trusted across a data environment or architecture. Further, every data call, transaction, or application call by a user or machine should be validated to ensure the requester has permissions to access the data.

This puts the question of IoT security front and center both for communication satellite providers but also for policymakers tasked with addressing this persisting and ever-growing area of national security concern.



Q4 - Supply Chains: Which, and How Many, Vendors Comprise the Satellite System's (Hardware and Software) Supply Chain?

The final category of concern focuses on the security and reliability of the supply chains that underpin satellite systems. In other words, how many suppliers and which suppliers make up a satellite system's supply chain and how has the satellite system provider sought to ensure the reliability of their systems given that supply chain? This category of national security concern was recently recognized in President Biden's February 2021 Executive Order on [Securing America's Critical Supply Chains](#): namely, that "production shortages, trade

There are two components to the supply chain conversation: availability and security. Availability, or reliability, refers to questions around access to particular vendors (hardware and software) and whether that access can reasonably be guaranteed. [...] In contrast, security of supply is focused on an assessment of the products themselves.

disruptions, natural disasters and potential actions by foreign competitors and adversaries" across critical supply chains can leave the United States deeply vulnerable ("Fact Sheet: Securing America's Supply Chains," 2021). In that context, for critical infrastructure, ensuring the availability and security of their suppliers is both a business and national security concern. In fact, both COVID-19 and the recent [semiconductor shortages](#) have demonstrated how fragile our supply chains can be (Griffith & Goguichvili, 2021).

There are two components to the supply chain conversation: availability and security. Availability, or reliability, refers to questions around access to particular vendors (hardware and software) and whether that access can reasonably be guaranteed. This category of supply chain concern focuses on potential choke points. Availability may be of concern if there are a limited number of vendors across or in a specific segment of the stack, if vendors

are geographically clustered, if vendors are located in a particularly unstable region or in an area where future conflict might erupt, or if vendors are untrusted (companies from countries with contentious relationships with the United States, for example) and may therefore reduce or deny access to products in the future.

In contrast, security of supply is focused on an assessment of the products themselves. One potential avenue through which insecurity can be introduced to a system stems from undue access (untrusted vendors within a supply chain). However, even if a vendor is not 'untrusted', they may still build out insecure products, products with shaky security foundations, or unintentionally provide a customer with products that have already been compromised. Unlike availability, which is concerned with maintaining access to certain products, security of supply focuses on how secure each component part of a system is and how companies verify the integrity of each of their component parts.

Notably, the particular shape and makeup of each supply chain will be largely provider specific, with some building out vertically integrated supply chains largely in-house and others integrating a disparate set of suppliers into their systems. SpaceX, for example, is primarily in-house from launch capabilities to the software running on their satellite systems on the ground and in space. In contrast, traditional GEO/GSO constellation



providers have historically not leveraged vertically integrated supply chains (single or in-house providers) and, instead, integrated a diversity of suppliers to build out their systems from launch to ground stations and from hardware to software.

It is also worth remembering that even if a provider has an entirely trusted supply chain (built largely in-house or from highly vetted vendors), it would be incorrect to then assume that they have fully addressed supply chain security concerns. This is true for physical infrastructure and data and digital systems security concerns as well, however. No single category is sufficient in isolation, and even with all three addressed at the cutting edge of best practices, defense is difficult and the threat environment constantly evolving.

Probing Questions:

1. *Do they have vendors within their system's supply chain who are introducing cybersecurity risk? If so, are there clear system boundaries which limit the access or visibility of those vendors components into the enterprise?*

This question requires an assessment of the vendors that make up the supply chain, but also who counts as an untrusted vendor (country of origin is one proxy but often overlooks broader sets of security concerns associated with vendors) and where replacements for those vendors might exist (if at all). Here, providers can speak to how they certify the security of specific vendors' components before deploying technology and how they address security concerns as they arise with suppliers once their products are already in use. From a national level, visibility into supply chains, such as a national review of the sector, would also shed light on the degree to which untrusted vendors occupy dominant or concerning positions in these systems, as well as the broader contours of the market (do any alternatives to those vendors exist).

Another question that is worth exploring is where we can architect around untrusted vendors in satellite systems and where we cannot. Put another way: at what level in the data transport stack are providers and operators of these systems concerned about supply-chain compromises? While the presence of untrusted vendors in geopolitically significant technology supply chains are an

important and pressing national security concern, it is also true that developing an entirely 'trusted' supply chain in every aspect of the satellite system stack may not be feasible for all industry players. This is the same concern that has arisen around 5G networks and Chinese vendors, with many European countries, for example, choosing not to ban Huawei and ZTE from their networks entirely but instead to limit where in the networks these systems can operate and then to focus on architecting around that risk. While the degree to which this is possible in 5G networks is still a live question, the same question should be asked of our satellite systems. Where can we architect around potential insecurity through the application of least trust principles, and where can we not?

While the presence of untrusted vendors in geopolitically significant technology supply chains are an important and pressing national security concern, it is also true that developing an entirely 'trusted' supply chain in every aspect of the satellite system stack may not be feasible for all industry players.



2. *Is the satellite system (from the ground-based assets to the space-based assets) characterized by a well-established development, security, and operations software and hardware pipeline with robust automated testing and deployment systems?*

If, for example, and returning to our conversation about defense-in-depth, they are using open-source software or commercial IT systems within any segment of their satellite system, what standard operating procedures have they put in place to ensure the security of that software when it is first acquired and deployed in their system, to actively monitor that software for vulnerabilities (utilizing both static and dynamic testing tools), to address vulnerabilities and areas of concern before they are exploited, and effectively respond if malicious activity is discovered? If they are using a closed ecosystem built specifically for the manufacturer's specifications, how are they assessing the security of those inputs?

Concerns around supply chain security are not merely theoretical. This attack vector was recently leveraged in the [SolarStorm campaign](#) (also sometimes referred to as the SolarWinds breach or Holiday Bear campaign) (Griffith, 2021b). Importantly, however, SolarStorm was not unique in that regard. Software supply chain compromises are not new; malicious actors have leveraged reliance on a variety of inputs into operations and systems before, including [NotPetya and Flame](#) (Herr et al., 2020).

3. *How many vendors make up their supply chains? And are their alternative vendors across the stack?*

[The terrestrial components of 5G networks](#) have been subjected to detailed supply chain reviews across the stack and numerous efforts to increase the diversity of players in that ecosystem (Griffith, 2021a). Notably, as those reviews revealed, the RAN is the least vendor-diverse part of the network. It also happens to be an area where the United States does not occupy a leadership position. More specifically, the United States does not currently have an equipment vendor that can manufacture radios at the scale necessary to meet the needs of the U.S. market, let alone a global market. This gap has led to significant public debate and policy attention (including a focus on [Open RAN](#) as one possible solution) (Griffith, 2020).

Yet, satellite systems have been largely absent from these supply chain reviews. A concerning oversight indeed given their growing role within 5G networks in particular and the important role they play in [supporting critical infrastructure and services](#) more broadly (King & Goguichvili, 2020). It is important to note, however, that supply chains in fairly niche markets are often far less diverse and robust than supply chains underpinning industries with far wider demand and profit-margins. Additionally, supply chains are complex and include everything from software to semiconductor chips and metal to rocket fuel.

Conclusion

Satellite systems are poised to play an ever-increasing role in telecommunications networks in general and 5G in particular. Importantly, this potential for greater integration between mobile networks and satellite systems would not even be a topic of conversation without three important, and fairly recent, shifts: (i) evolving satellite system technology and (ii) the development of new business models coupled with (iii) increasing demand for bandwidth. These three shifts are redefining the relationships at the heart of our telecommunications networks and vastly



increasing both the threat surface and the density of the data. This places satellite systems in the middle of national security concerns associated with 5G networks.

Yet, despite the recognition that 5G networks will represent an increasingly critical infrastructure and that investing in the security, resilience, and defensibility of 5G networks is, therefore, a national security imperative, much of the focus to-date has been on the terrestrial components of these networks. This leaves an important and concerning gap in the broader 5G and national security conversation that needs to be filled for the United States to successfully balance the promise and the peril of these networks now and in the future.

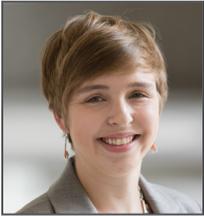
We cannot adequately assess and address national security concerns associated with 5G networks without also considering the space-based components of these networks now and in the future. And deeply concerning, the security, resilience, and definability of space-based systems has all too often been historically overlooked and poorly understood in policy circles.

Importantly, as we begin to fill this gap, we must avoid the misperception that in space, everything is different. Many of the critical infrastructure concerns we have with the terrestrial components of 5G networks carry over to our conversations about the satellite system components of these networks. We can and should lean on those hard learned lessons, while adjusting our answers to the realities of space. The four questions and their subsequent probing question outlined here serve as both an overview of the type of national security considerations that need to be addressed and as an opportunity of the policy community, satellite system providers, and satellite system users to collaborate on potential paths forward.

In summary, satellite systems require additional scrutiny and consideration. Why? These systems will continue to play an increasingly important role within critical infrastructure and in support of critical services. As a consequence of the scale and scope of their importance, they will also continue to be the targets of geopolitical rivals and competitors. Yet, these systems have been largely overlooked in the United States' broader 5G security efforts: from the availability and security of supply chains to shared responsibility models and from defense-in-depth to base-stations as strategic assets. While it would have been better to have historically and robustly invested in the security, resilience, and defensibility of these systems, it behooves us to correct that oversight today to best equip ourselves for the future.



About the Authors



Melissa K. Griffith is a Senior Program Associate with the Science and Technology Innovation Program (STIP) at the Woodrow Wilson International Center for Scholars; a Non-Resident Research Fellow at the University of California, Berkeley's Center for Long-Term Cybersecurity (CLTC); and an Adjunct Professor at Georgetown's Center for Security Studies (CSS). She works at the intersection between technology and national security with a specialization in cybersecurity, semiconductors, and 5G networks. Her work sheds important light on the components and dynamics of cyber power and cyber conflict, as well as the vital role that public-private cooperation and both security and economic policy play in national defense. Prior to joining the Wilson Center, Griffith was a Pre-Doctoral Fellow at Stanford University's Center for International Security and Cooperation (CISAC) and a Visiting Research Fellow at the Research Institute on the Finnish Economy (ETLA) in Helsinki, Finland. Griffith holds a Ph.D. and an MA in Political Science from the University of California, Berkeley and a B.A. in International Relations from Agnes Scott College.



Christopher M. Hocking is the Executive Director and President of the Cyber Conflict Studies Association and an active-duty Air Force officer assigned to Headquarters, Department of the Air Force serving on the Air Staff. He received a Bachelor of Science in Political Science from the United States Air Force Academy and a graduate degree from the University of Virginia. He leads Air Force programs of record as a program manager, served as an executive officer, led a multi-disciplinary team on an inter-agency program, and supported security operations while deployed in Afghanistan. He has broad programmatic and systems engineering experience in data analytics, cloud computing, communications, weapon-system software development and integration, cyber capabilities, command and control systems, and multi-domain and Joint Operations. Prior to assuming his current position, Hocking was the Executive Officer and Assistant Professor of Political Science at the U.S. Air Force Academy. He has affiliations with the U.S. Air Force Academy's Eisenhower Center for Space and Defense Studies and Air Force CyberWorx.

The views expressed are those of the authors and do not reflect the official guidance or position of the United States Government, the Department of Defense or of the United States Air Force.



References

- About - Hubble Servicing Missions*. NASA. (2021, January 15). https://www.nasa.gov/mission_pages/hubble/servicing/index.html.
- Amazon. (2021). *AWS Ground Station*. Amazon Web Services (AWS). <https://aws.amazon.com/ground-station/>.
- Bailey, B., Speelman, R. J., Doshi, P. A., Cohen, N. C., & Wheeler, W. A. (2019, November). *Defending Spacecraft in the Cyber Domain*. The Aerospace Corporation. https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf.
- Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. Harvard University Press.
- Challenges to Security in Space*. Defense Intelligence Agency. (2019, February 11). <https://media.defense.gov/2019/Feb/11/2002088710/-1/-1/1/SPACE-SECURITY-CHALLENGES.PDF>.
- Committee on National Security Systems. (2016, May 6). *Policies*. <https://www.cnss.gov/CNSS/issuances/Policies.cfm>.
- Critical Infrastructure Protection: Commercial Satellite Security Should be More Fully Addressed*. United States General Accounting Office. (2002a, August). https://www.google.com/books/edition/_/kIYBpOci46EC?hl=en&sa=X&ved=2ahUKEwj4pYC8g-jxAhX3EFkFHeKFDPAQ8fIDMA16BAgHEAQ.
- Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed*. U.S. Government Accounting Office. (2002b, August 30). <https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-02-781/html/GAOREPORTS-GAO-02-781.htm>.
- Crossely, G., Jones, G., & Blanchard, B. (2020, January 6). *China eyes increased ties with Kiribati, site of space tracking station*. Reuters. <https://www.reuters.com/article/us-china-kiribati/china-eyes-increased-ties-with-kiribati-site-of-space-tracking-station-idUSKBN1Z5168>.
- Daehnick, C., Klinghoffer, I., & Wiseman, B. (2020, May 4). *Large LEO satellite constellations: Will it be different this time?* McKinsey & Company. <https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/large-leo-satellite-constellations-will-it-be-different-this-time>.
- Embracing a Zero Trust Security Model*. National Security Agency. (2021, February). https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF.
- Fact Sheet: Securing America's Critical Supply Chains*. The White House. (2021, February 24). <https://www.whitehouse.gov/briefing-room/statements-releases/2021/02/24/fact-sheet-securing-americas-critical-supply-chains/>.
- Flexible Payloads*. Airbus. (2021). <https://www.airbus.com/space/telecommunications-satellites/flexible-payloads.html>.
- Foust, J. (2021, March 11). *SpaceX launches Starlink satellites and expands international service*. SpaceNews. <https://spacenews.com/spacex-launches-starlink-satellites-and-expands-international-service/>.
- Gibson, C. (2018, June 11). *IoT and Satellite Security in the Age of 5G*. Trend Micro. https://www.trendmicro.com/en_us/research/18/f/attack-vectors-in-orbit-need-for-satellite-security-in-5g-iot.html.
- Griffith, M. K. (2019, November). *5G and Security: There is More to Worry about than Huawei*. The Wilson Center. <https://www.wilsoncenter.org/publication/5g-and-security-there-more-to-worry-about-huawei>.
- Griffith, M. K. (2020, November 2). *Open RAN and 5G: Looking Beyond the National Security Hype*. The Wilson Center. <https://www.wilsoncenter.org/article/open-ran-and-5g-looking-beyond-national-security-hype>.
- Griffith, M. K. (2021 (a)). *Balancing the Promise and the Peril of 5G: The State of Play in the United States*. The Wilson Center. <https://5g.wilsoncenter.org/publication/balancing-promise-and-peril-5g-state-play-united-states>.
- Griffith, M. K. (2021 (b), April 26). *In the Wake of SolarWinds, the U.S. Must Grapple with the Future and Not Just the Past*. Lawfare. <https://www.lawfareblog.com/wake-solarwinds-us-must-grapple-future-and-not-just-past>.
- Griffith, M. K., & Goguichvili, S. (2021, March 23). *The U.S. Needs a Sustained, Comprehensive, and Cohesive Semiconductor National Security Effort*. The Wilson Center. <https://www.wilsoncenter.org/blog-post/us-needs-sustained-comprehensive-and-cohesive-semiconductor-national-security-effort>.
- Hack-A-Sat*. The United States Air Force and United States Space Force. <https://www.hackasat.com/>.



- Harrison, T., Johnson, K., & Young, M. (2021, February 25). *Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons*. Center for Strategic & International Studies. <https://www.csis.org/analysis/defense-against-dark-arts-space-protecting-space-systems-counterspace-weapons>.
- Henry, C. (2020, July 30). *Amazon's Kuiper constellation gets FCC approval*. SpaceNews. <https://spacenews.com/amazons-kuiper-constellation-gets-fcc-approval/>.
- Herr, T., Loomis, W., Scott, S., & Lee, J. (2020, June 26). *Breaking trust: Shades of crisis across an insecure software supply chain*. Atlantic Council. <https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/>.
- Hollingham, R. (2013, June 9). *What would happen if all satellites stopped working?* BBC. <https://www.bbc.com/future/article/20130609-the-day-without-satellites>.
- Hunt, B. (2012, September). *An approach to Return on Investment (ROI) for Independent Verification and Validation (IV&V) at NASA*. Slide 1. https://www.nasa.gov/sites/default/files/1-4a-ivv_conference_bob_hunt_dulos_kalman.pdf.
- iDirect SatHaul-XE™ Overview*. iDirect. <https://www.idirect.net/wp-content/uploads/2019/01/SatHaul-XE-Solution-Overview-2018.pdf>.
- Informa PLC. (n.d.). *Whispers Among the Stars: A Practical Look at Perpetrating (and Preventing) Satellite Eavesdropping Attacks*. Black Hat. <https://www.blackhat.com/us-20/briefings/schedule/index.html#whispers-among-the-stars-a-practical-look-at-perpetrating-and-preventing-satellite-eavesdropping-attacks-19391>.
- Information Sharing and Analysis Center*. Space ISAC. (n.d.). <https://s-isac.org/>.
- Jones, M. (2016, October 18). *Ground control of space is highly political*. The Interpreter. <https://www.lowyinstitute.org/the-interpreter/ground-control-space-highly-political>.
- King, M., & Goguichvili, S. (2020, October 8). *Cybersecurity Threats in Space: A Roadmap for Future Policy*. The Wilson Center. <https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy>.
- Lee, R. M. (2015, September 1). *The Sliding Scale of Cyber Security*. Sans. <https://www.sans.org/white-papers/36240/>.
- Lockheed Martin And Omnispace Explore Space-Based 5G Global Network*. Lockheed Martin. (2021, March 23). <https://news.lockheedmartin.com/5g-omnispace-agreement>.
- Low Earth orbit*. The European Space Agency. (2020, March 2). https://www.esa.int/ESA_Multimedia/Images/2020/03/Low_Earth_orbit.
- Mosher, D. (2016, November 16). *SpaceX just asked permission to launch 4,425 satellites — more than orbit Earth today*. Insider. <https://www.businessinsider.com/spacex-internet-satellite-constellation-2016-11>.
- National Coordinating Center for Communications*. Cybersecurity & Infrastructure Security Agency. (n.d.). <https://www.cisa.gov/national-coordinating-center-communications>.
- Protecting America's Global Positioning System*. U.S. Department of Defense. (n.d.). <https://www.defense.gov/Explore/Spotlight/Protecting-GPS/>.
- Sheetz, M. (2021, April 19). *Amazon signs with ULA for rockets to launch Jeff Bezos' Kuiper internet satellites*. CNBC. <https://www.cnbc.com/2021/04/19/amazon-signs-ula-rockets-to-launch-bezos-kuiper-internet-satellites.html>.
- Sheetz, M. (2021, March 23). *Lockheed Martin partners with satellite start-up Omnispace to build a space-based 5G network*. CNBC. <https://www.cnbc.com/2021/03/23/lockheed-martin-partners-with-omnispace-for-satellite-5g-network.html>.
- Thompson, A. (2021). *SpaceX launches 60 new Starlink internet satellites, nails latest rocket landing at sea*. Space.com. <https://www.space.com/spacex-starlink-22-satellites-launch-rocket-landing-success>.
- UCS Satellite Database*. Union of Concerned Scientists. (2021, May 1). <https://www.ucsusa.org/resources/satellite-database>.



WOODROW WILSON INTERNATIONAL CENTER FOR SCHOLARS

The Wilson Center, chartered by Congress in 1968 as the official memorial to President Woodrow Wilson, is the nation's key non-partisan policy forum for tackling global issues through independent research and open dialogue to inform actionable ideas for the policy community.

THE SCIENCE AND TECHNOLOGY INNOVATION PROGRAM (STIP)

The Science and Technology Innovation Program (STIP) brings foresight to the frontier. Our experts explore emerging technologies through vital conversations, making science policy accessible to everyone.

Copyright © 2021 by The Wilson Center

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027

The Wilson Center

-  www.wilsoncenter.org
-  wwics@wilsoncenter.org
-  facebook.com/woodrowwilsoncenter
-  [@thewilsoncenter](https://twitter.com/thewilsoncenter)
-  202.691.4000



STIP

-  www.wilsoncenter.org/program/science-and-technology-innovation-program
-  stip@wilsoncenter.org
-  [@WilsonSTIP](https://twitter.com/WilsonSTIP)
-  202.691.4321

