NSR
NORTHERN SKY RESEARCH

# Space Cybersecurity

## Current State and Future Needs

April, 2022

# ABSTRACT


As the global economy is more dependent on space resources, devices and inter-linked networks, the need to proactively address the exposure to new cyber-threats increases. Innovation-fueled growth in space, and shifts in value chains interworking with terrestrial, wireless and cloud ecosystems goes in parallel with hackers' increased capabilities of finding vulnerabilities in the infrastructure.

What needs to happen is a complete paradigm shift around how to address cybersecurity threats in space systems. Traditional cybersecurity techniques focused on perimeter defense, access control and accountability are no longer sufficient to prevent cyber breaches, including insider threats. The space cybersecurity model must shift to a Zero Trust Architecture, which will continuously question the security, vulnerability, and reliability.

This white paper explores the unique needs of the space sector and satellite networks, the challenges brought by new disruptions and the solutions available around the key concept of Zero Trust Cybersecurity.


*Satellite industry stakeholders must shift from perimeter security to a "Zero Trust" strategy:*

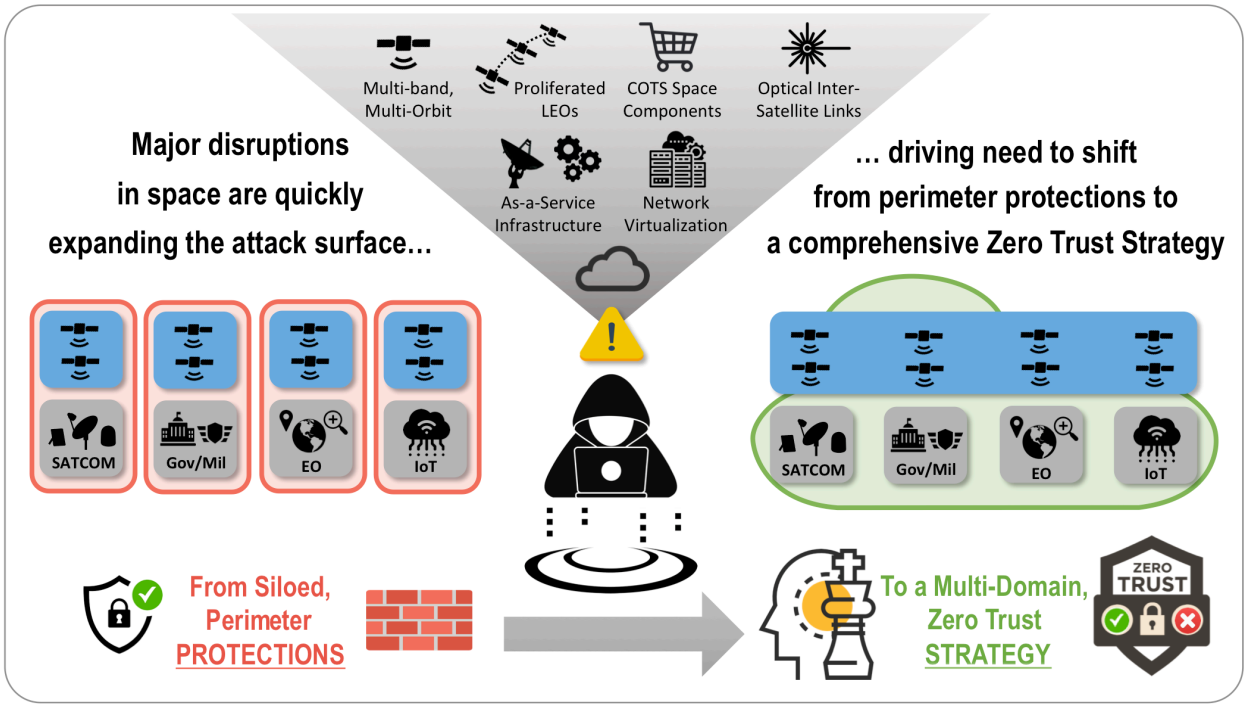
*Enforce least privilege, per-request access to information systems, network devices and applications.*

# Table of Contents

# Executive Summary

It is no secret that space is experiencing unprecedented transformations. More satellite constellations are being built than ever before, deployed across different orbits and using multiple frequency bands in support of myriads of applications, both commercial and military. As the global economy is ever more dependent on satellite data, services and devices from satcom, earth observation and IoT networks interplaying with cloud ecosystems, the need to minimize the exposure to increasingly sophisticated cyber-threats becomes clear.

NSR[1] projects from 2020 to 2030 the satellite and space sector will yield $1.2 Trillion in Retail Revenues, see over 24,850 satellites launched into space, and generate more than 504,000 petabytes in data volume. These are seismic-shift of industry activity compared to the previous ten years – and is only expected to accelerate in the decades to come. Disruptions not only foster growth but also expand the attack surface, prompting players to re-assess security practices.




*Source: NSR*

While the past decades have been built around siloed stovepipes of infrastructure where location conveys security – these ten years and the ten years after next will require a complex mix of infrastructure ownership models to unlock the 'next Trillion' in revenues. Scaling beyond the current paradigm to unlock the next-set of use cases will require significant investments in space and on-earth – and require a different concept of ownership. Already, the US Government is moving towards leveraging more commercial sources of space-based resources from connectivity infrastructure to Earth Observation and Analytics. Commercial players are expanding their services-based business models, mirroring terrestrial as-a-service plays in response.

Scaling these business models in the context of an increasing attack surface requires new solutions because traditional cyber protections, while useful, are no longer sufficient. A shift from traditional

[1] https://www.nsr.com/?research=nsr-global-space-economy-2nd-edition

protections to a Zero-Trust strategy is required. Zero Trust Architectures (ZTA) minimize and contain security risks by making inter-connected networks far more resilient.

# Introduction: Shifting Space Supply Chains

The space industry has been expanding at a rapid pace, with thousands of satellites launched over the past decades and many thousands more launching. Disruptions challenge traditional satellite supply chains and bring a new set of security challenges. The increasing commercialization of the sector has built a very large pool of actors across the globe. A more competitive environment has brought in more competitive technologies, pushing companies to diversify and expand their footprint across verticals. Several mergers and acquisitions have taken place in recent years, and more companies have started manufacturing in-house. The pandemic reinforced these trends, and the space industry shifted into a complex environment where the security of space data and systems is inter-dependent with satellite operators, carriers, and satellite manufacturers.

An "abundance paradigm" of high-bandwidth space assets, software-defined networking, and cloud-empowered services and applications is replacing satellites' historical scarcity economics and monolithic islands of technologies. The new paradigm is characterized by a diversity of players gravitating towards network collaboration via enabling layers with software programmability across multi-domain, network-as-a-service implementations. The various applications and respective supply chains are being affected differently; with key implications including:

- **Earth Observation Players:** EO operators that roll out dedicated business lines or make acquisitions (horizontal, as with Planet and Vandersat, or vertical, as in the case of Maxar) tap into the big data analytics market; while ground station service providers are working in tandem with cloud computing players to provide integrated on-demand access to data from end-to-end. Major cloud computing players like Amazon and Microsoft are themselves injecting efficiencies into the EO ecosystem by deploying or fostering the deployment of ground stations to be leveraged on demand via programmable, as-a-service business models that interplay with their cloud computing ecosystems.

- **Satcom Players:** Satellite operators and service providers may move up and down the value chain to remain competitive and capture growth, while –simultaneously- they increasingly rely on software-enabled service extensions in collaboration with partners such as cloud providers. Some major players have made vertical acquisitions to tap into larger addressable markets (such as Intelsat and Gogo) while others are considering or executing on horizontal integration strategies, such as the Viasat-Inmarsat merger. Yet, changes in satcom are multi-level, with other trends including:
    - Service providers and telcos partnering with satellite manufacturers to own partial payloads (i.e. hosted payloads) or full satellites, without flying the satellites themselves. The Anuvu purchase of Astranis Micro-GEO satellites to provide in-flight connectivity for airlines is a prime example.
    - GEO satellite operators evaluating orchestrated multi-orbit complementation opportunities with MEO and LEO systems
    - Traditional and new players exploring multi-orbit link relay opportunities to mitigate or eliminate the space-to-ground bandwidth bottleneck of LEO Earth Observation constellations.

- **Military & Government:** Traditional government and defense operators are making a concerted effort to increase reliance on the commercial sector to tap into the opportunities

provided by an abundant array of space assets and network solutions across different orbits and frequency bands: The SDA[2]'s Transport Layer and its push for interoperable constellations is a prime example. As the line between commercial and GovMil system blurs, it naturally becomes imperative for next gen satellite solutions to adhere to updated security standards – as with the US DoD[3]'s recently launched CMMC[4] 2.0.

- **Satellite Manufacturers:** As satellite manufacturers put emphasis on manufacturing and delivering software-defined satellites, their business models can also shift towards software capabilities that can be enabled and reconfigured based on as-a-service licensing and operating conditions. Modifying spectrum, spectral power and beam shape and/or steerability on high throughput satellites via dynamic operations control can drive performance enhancements while avoiding interference.

- **In-Orbit Services (IoS):** The satellite industry will remain torn between investment in replacements, flying them longer in inclined orbit versus improved flexibility once on-orbit such as the MEV life extension missions from Northrop Grumman. However, as the industry moves towards addressing demand of custom services at a increasingly competitive prices, it becomes vital for IoS service providers to diversify the IoS applications offerings and to collaborate on sharing best practices, developing technical and safety standards, and establishing clear expectations of outer-space operations.

Therefore, depending on the customer requirements, the value chain has discretized itself into various as-a-service offerings, from Ground-Stations-aaS to Data-Infrastructure-aaS. In each of these cases, the complexity of the ecosystem is expected to increase, and along with it, potential security risks – from the end-to-end integrity of data to cyber-attacks at vulnerable access points across the network. In the wake of such changes in the space supply chain landscape, it is critical for space industry vendors and solution providers to upgrade existing risk assessment and vulnerability scan paradigms.

# Security Problems In Space

## The Augmented Challenges of New Space and Proliferated LEOs

Traditional cybersecurity encompasses the principles of perimeter defense, access control and accountability, all focused on protecting internal resources from outside threats. Essentially, entities independently build protective walls around their infrastructure to safeguard systems and data from theft and manipulation. Some of the best-known methods of doing this are the use of encryption, passwords, anti-virus, and security compliance.

[2] Space Development Agency (SDA)

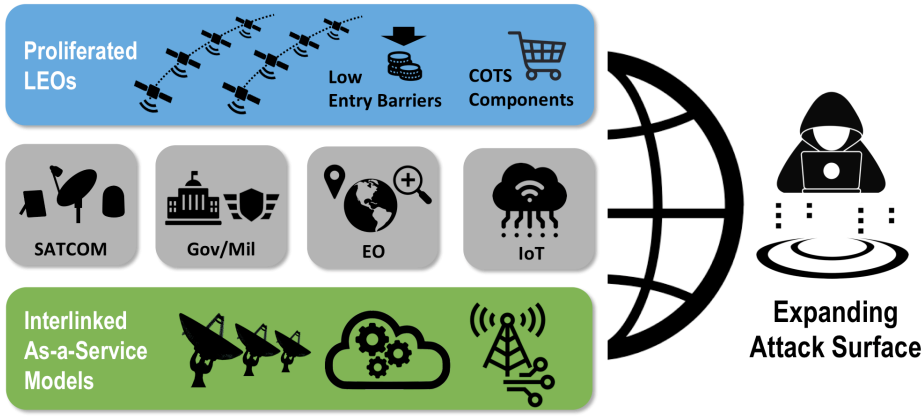
[3] U.S. Department of Defense (DoD)

[4] Cybersecurity Maturity Model Certification (CMMC)

With technological advancements taking place in an increasingly heterogeneous and multi-disciplinary environment, those traditional cybersecurity methods are no longer sufficient to prevent cyber breaches from happening. Worse yet, when breaches do occur, because of today's software-centric characteristics of dynamic networks, such breaches can be used as springboards for damage amplification. What needs to happen is a complete paradigm shift around how to deal with cybersecurity threats; moving away from perimeter security measures and technologies to a comprehensive and evolving cybersecurity strategy. While perimeter security devices such as Type-1 encryptors, are very reliable because they are controlled by very strict requirements, they do not constitute a complete strategy by themselves.


Cyber-attacks on satellites and space-based systems have indeed occurred on multiple occasions[5]. Some of these attacks were carried out through the ground station, whereas others were targeted directly at disturbing the signal transmission of satellites, or even at causing physical damage to a satellite. Today's proliferation of connectivity and interdependence of distinct applications, and across heterogeneous security networks, opens new doors for cybercriminals to hack devices to then move laterally to manipulate the data.

Cyber-attackers can operate from anywhere and have different objectives – from malware/ransomware attacks against end-users looking for financial gains to infrastructure disruption or denial of service as part of a larger conflict. Two key recent technological advancements in space networks highlight the importance of adopting more resilient cybersecurity strategies:




*Source: NSR*

- **More COTS Components:** Earth Observation and Communications satellites are vulnerable to attacks, especially commercial proliferated LEO[6]s as manufacturers increasingly use Commercial Off The Shelf (COTS) technologies and components that do not have a strong security element integrated.
- **Increasing Software Focus:** Advancements in digital ground networks and software-defined networks with increasing levels of flexibility, programmability and automation are becoming vital for solving scalability constraints in EO and satcom. Yet, ground networks' reliance on smart software and interdependencies with terrestrial networks and cloud extensions, make such networks more susceptible to attacks.

[5] Hackers could shut down satellites – or turn them into weapons https://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932#:~:text=A%20history%20of%20hacks,panels%20directly%20at%20the%20sun.

[6] Low Earth Orbit (LEO)

These trends become particularly critical in proliferated LEO scenarios, comprising hundreds or thousands of satellites interacting with tens or hundreds of ground network nodes, or –ultimately- millions of electronically-steered user antennas or IoT devices. While such technological evolutions around COTS components and software-centric systems are positive in terms of fostering cost reduction and value creation, they also have the net effect of expanding the attack surface for cybercriminals to exploit. A good example of what can happen when the attack surface is drastically expanded can be taken from the infamous Mirai Internet of Things (IoT) botnet, which in 2016 took down major websites using hundreds of thousands of compromised IoT devices. Mirai was possible because IoT developers did not focus design requirements around security for their low-cost, widely deployed products. Even today, botnets built from the Mirai codebase continue to threaten networks and systems, as cyberattackers leverage lax Internet of Things (IoT) security in legacy, low-cost devices to conduct widespread attacks.

In all, the entire space and satellite sector must view cybersecurity as an evolving landscape of best-practices and solutions rather than a static state which is measured and monitored. The evolution in network architectures with complex interworking and business relationships from WAN to LAN and edge devices is not unique to satellite networks. Space shares commonalities with other sectors providing similar services wirelessly or terrestrially, but satellite networks also have inherent characteristics that make security[7] even more sensitive to attacks:

> *"You cannot expect cyber products designed for terrestrial operations to meet the extreme requirements of securing assets in space"*[7]

**Dave Pearah**
CEO, SpiderOak

- **Wide Coverage:** Satellites cover large surface areas either statically or dynamically, thus naturally exposing large surfaces of attack at the RF level. While in terrestrial networks, connection hops could be traced down to specific devices and locations, in satellite it may be difficult to granularly spot specific locations of attack antennas. RF signal triangulation techniques can reduce the uncertainty but nevertheless it is difficult to pinpoint and cancel specific attack locations promptly. Furthermore, the attack location could move. Risk applies to any type of satellites, orbits and frequency bands. In LEO orbits, satellites have a smaller visibility of the Earth's surface but telemetry & command may be performed over specific windows of visibly between each satellite and TT&C stations, thus opening time windows for malicious attacks.

- **Limited In-Space Repair:** Unlike terrestrial and wireless networks, at the time of this white paper writing, the industry capabilities to repair intentionally damaged satellites or malfunctions are very limited. In a worst-case scenario, a cyber-attack on a space-based system or component could destroy an entire satellite, leading to financial losses of millions of dollars for the operators and its clients and stakeholders.

- **Cascading Risk:** Once an attacker gains control over a satellite, lateral movements can result in rather catastrophic events not only for the specific network but for the entire space sector. As an example, for LEO satellite constellations with satellite cross-links, the entire

[7] SpiderOak CEO Dave Pearah on Mornings With Maria, Fox Business https://www.youtube.com/watch?v=b2sfNZICxGo

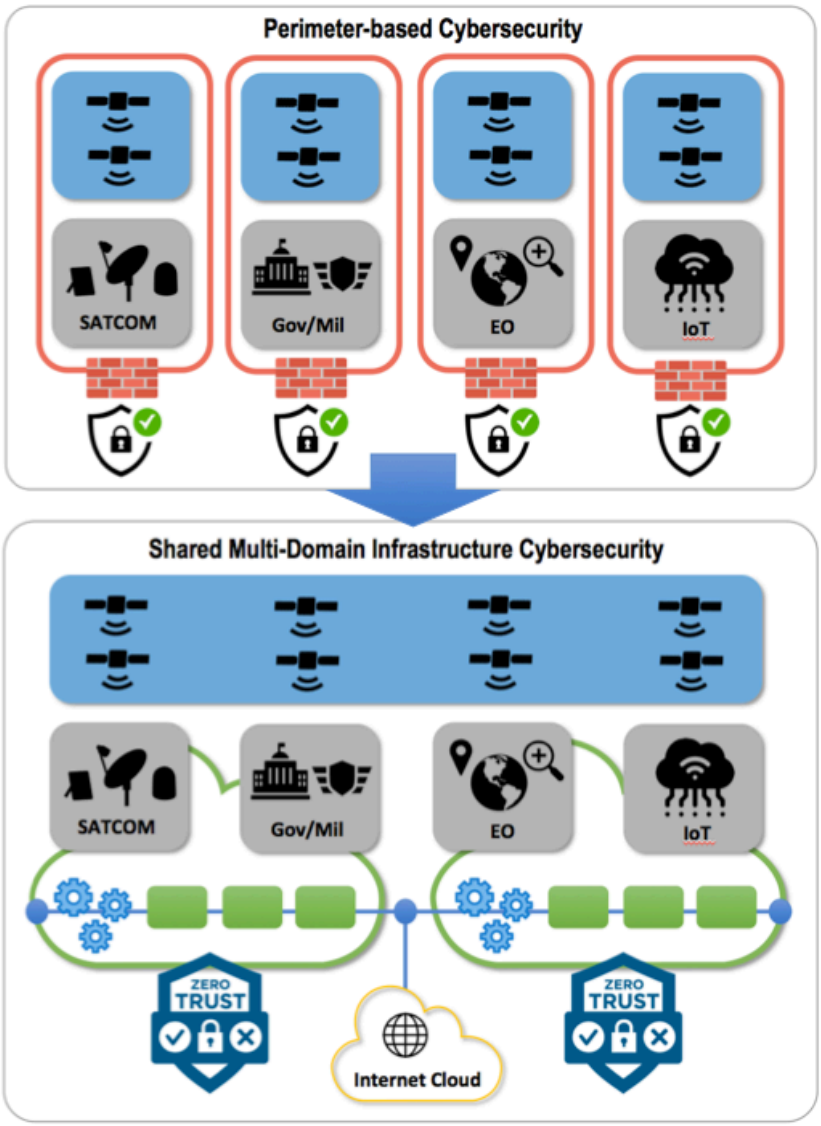
constellation system could be compromised in space without need to relay signals back the ground network. A proliferated LEO environment is also increasingly becoming susceptible to cascading collisions among satellites and space debris, potentially making certain altitudes unusable for years.

- **Third-Party Facilities:** Satellite networks are increasingly more heterogeneous and complex requiring gateway systems to be deployed at third party facilities including but not limited to telecom operators, teleport operators, service providers or even datacenters. These gateway stations naturally traverse a wide array of terrestrial networks with their own vulnerabilities, spanning from dark fiber to IP transit networks. Insider threats and human errors also increase in the context of multi-level access of multiple operation centers.

# The Zero Trust Solution Framework

## The Ownership = Control (and Security) Paradigm

Infrastructure ownership has traditionally been a core facet of value-creation in the Satellite & Space markets. Satellite Operators build-out a complex network of space-based hardware and ground-based networks to deliver connectivity to the furthest corners of Earth. Government and Militaries build their own satellite networks to further this notion that, to have control one must have ownership. Together, security occurred at the edge of the network through perimeter defense via firewalls, air gaping, and other 'hard outside' type security best-practices. Overall, this ownership-enabled security paradigm served the Satellite and Space sector well with few public cyber security breaches or other major events.




*Source: NSR*

Move forward to today, and the threat plane has increased significantly – not only is the concept of ownership rapidly evolving but the barriers of physical or cyber security events have decreased significantly. No longer does the obscurity of space-based infrastructure or security through perimeter defense enable a truly secure environment. RF Jamming on both commercial and military networks enabling connectivity or Earth Observation applications

have increased significantly over the past few years, with the notable public example of GPS spoofing in the South China Sea. On the cyber-security front, individuals can leverage significant tools and capabilities to disrupt nation-states in a tit-for-tat battle where legitimate users get caught-up in the middle of these cyber instances. Space-based assets are no longer immune from these threat vectors as the industry looks to 'act more' like terrestrial infrastructure and applications

Satellite and Space players have not been idle amongst this changing threat paradigm – yet, they can still do more to leverage best-practices. An emerging paradigm of cyber-security frameworks focused on the unique features and characteristics of the space industry helps. Risk-based frameworks from organizations such as the US National Institutes of Standards and Technology (NIST) NIST 800-53, IA-Pre by US Space Force focused on Commercial Satellite Communications (COMSATCOM) security evaluation, and other policies around the globe are helping to build a more secure future. However, they largely operate in the ownership yields control and control yields security paradigm.

Simply, although the underlying infrastructure may no longer be owned by the organization providing the service it is still sliced and segmented into virtual networks. While firewalls leveraging intrusion detection/protection/etc. systems (IDS), traffic shaping/profiling, real-time threat analysis leveraging AI/ML all qualify as best-practices it is largely built around a concept of 'if you are inside then you are approved.' Instead, as the concept of ownership migrates from physical assets to 'virtual slices' and quickly towards "X-as-a-service" session-based capabilities so too must the concept of security within the Satellite and Space sector.

## Zero Trust Principles

Given the complexities associated with the new satellite paradigm, building higher walls to stop malicious actors at the gate no longer scales as it has become an exponentially growing and complex problem to even define perimeters.

This is pushing the entire industry to move away from perimeter security towards a Zero-Trust security strategy[8], with the inherently embedded principle that system stakeholders must never grant implicit trust to partners, users, devices or applications based solely on their properties such as satellite or network location. Leading stakeholders such as the US Department of Defense (DoD) are taking space into consideration while developing a zero-trust security framework.

Following IBM's Zero Trust Architectural framework[9], ZTA strategies must comply with three basic principles:

1. **Never Trust, Always Verify:** Every time a user, device or application tries to make a new

> *"How does zero trust relate when we're talking about things in orbit? I think it relates in many ways"*[8]

**John Sherman**
U.S. Department of Defense
Chief Information Officer

[8] Space is a critical part of DOD's move to zero trust https://www.fedscoop.com/space-is-a-critical-part-of-dods-move-to-zero-trust-cio-says/

[9] https://www.ibm.com/security/zero-trust?utm_medium=OSocial&utm_source=Youtube&utm_content=000023UA&utm_term=10010612&utm_id=YTDescription-Zero-Trust-Solution-Page

connection attempt, such attempt should be rigorously authenticated and authorized, even if it comes from inside the network or via trusted partners.

2. **Least Privilege:** Users and applications must be granted only the minimum amount of access needed, as needed and dynamically to perform their respective tasks.

3. **Assumed Breach:** Networks security must assume that breaches will always occur, thus be planned for worst-case scenarios so that the architecture, when built around a robust and tested incident response, behaves like an immune system.

These principles when well planned and implemented have the effect of shrinking the attack surface and that, when breaches do occur, the implications are contained because the entire system is resilient, behaving similarly to an evolving immune system.

## The Air Travel Analogy

In the "golden age" of air travel, passengers could walk straight on to an airplane with few questions around if they 'really belonged' –presence at the airport was enough. Move forward a few years, and gate agents checked tickets to ensure passengers were at the right flight. Presence and ticket check for many years was sufficiently secure. 9/11 changed that paradigm – introducing another layer of perimeter defense but adding ID verification and other security processes. Today, air travel security is a complex mix of perimeter defense, ID security, and most importantly – removing a concept that location can confer trust. Simply being present at an airport can no longer enable 'getting on an airplane.'

The evolution of air travel security is a prime example of building a zero-trust framework. Expanding that analogy to other airport services - duty-free purchases require authentication (via ticket), access to an airport lounge requires another authentication process (via airline status/relationship), and other services are frequently built around more than just location-based authentication, but instead identity-based security. So air travel is now built around the concept of "Don't trust, verify". After verification, enable service.

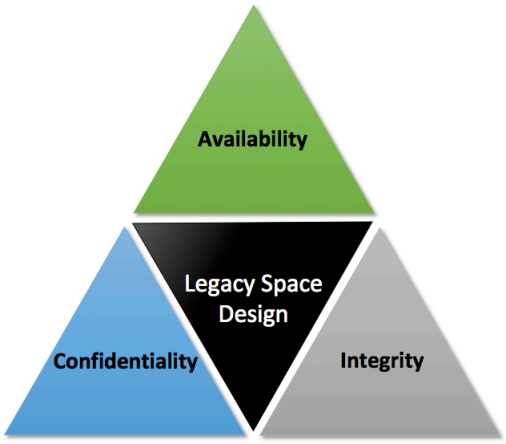
Satellite and Space players are following a similar development pathway – just as airline passengers are in the 'travel-as-a-service' shared infrastructure model with ticket-based authentication – the space industry is moving from owned to shared ownership paradigms. Don't trust that application inside the firewall, verify.

Moreover, the concept of Zero Trust is gaining adoption throughout the security community. Just as NIST 800-53 builds out a risk-based assessment framework NIST 800-207, uses zero-trust principles to plan industrial and enterprise infrastructure and workflows. While "Satellite" does appear in section 4.1 of NIST 800-207 it does not directly mean 'something in outer space.' Building and deploying these zero-trust concepts into operational satellite and space networks will require a re-evaluation of how security through location can evolve into "Don't Trust – Verify".

## The Availability-Integrity-Confidentiality Triad

Traditional information security paradigms typically revolve around the "CIA Triad" – Confidentiality, Integrity, and Availability (CIA). In the Space & Satellite sectors, the implementation of these three points have focused on availability – redundant TT&C infrastructure, primary and secondary onboard mission control processors, and other design decisions which reflected a key fact of legacy space – it

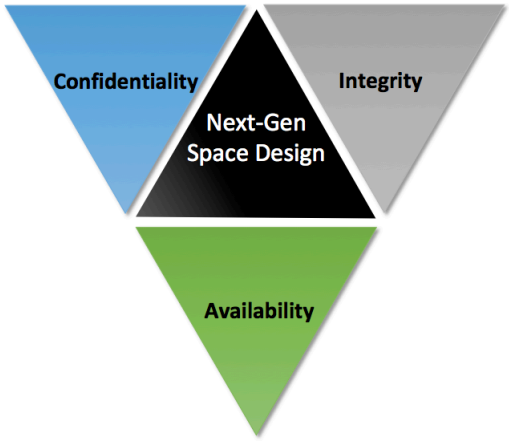
was expensive to get there and took a while to build/launch/repeat – frequently measured in decades and taken hundreds of millions of dollars to achieve.




This concept of operations whereby availability is paramount is true across civil, commercial, and military space. JP 3-14 from the US Department of Defense encapsulate this thinking best, where the term 'availability' appears throughout the document, but most directly it states the Combined Space Operations Center (CSPOC) goal as, "Ensures optimization and availability of critical space services to support global users." In that environment, making sure 'things worked' was paramount. In short, networks from the spacecraft downward were designed around availability as measured from the control plane and the 'mission to end-user'.

The availability-focused paradigm of Space & Satellite markets is changing – as access to space becomes cheaper, onboard capabilities increase, and availability frequently means leveraging a complex mix of owned and shared infrastructure models. This means the Confidentially, Integrity and Availability triad is flipping. No longer can space-based assets rely entirely on closed-architectures with bespoke ground-based control planes. Integrity of the actual mission data is becoming front of mind as PNT jamming/spoofing/denial increases throughout the world. Military and commercial operators are right now planning for the 'what-ifs' which include more sophisticated spoofing into the data layer itself – exploiting the increasing threat plane to manipulate or deny space-based assets at critical moments in time. Today, integrity of control and mission payload data is the emphasis.

To implement this integrity-optimized doctrine, hardened operating systems such as TriSept's hardened Linux operating environment are proliferating. The OS uses more terrestrial-like security practices with an emphasis on zero trust – in essence optimizing for the integrity the system because availability is a given – those offering low availability are simply not in the market. Most recently, SpaceX's Starlink network operating in Ukraine has found that integrity (in this case resilience against jamming) is as critical as more traditional availability metrics – landing right, terminals in-country, etc. While jamming could be considered a traditional availability metric – the mere presence of jamming indicates that availability alone is no longer the variable of optimization. Instead, the integrity of the service must coexist alongside the legacy concepts of availability.




Overall, as more shared infrastructure models proliferate across the space domain – both on orbit and on the ground – thinking must shift from availability-most, to a holistic integrated approach to security and design. Integrity is frequently built off of availability, and availability is 'table stakes' in this sector. The next-era of space-focused products and services must adapt beyond unscalable models of bespoke ground control infrastructure, customized onboard processing/operating systems, and instead operate in an era where trust is constantly questioned – in a zero trust architecture.

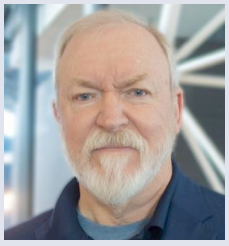
## Industry Solutions: Unlocking Value Without (End-to-End) Ownership

Looking back at the air travel experience, the next-generation of passenger experience is enabled by zero-trust identity verification. Onboard purchasing is going card-less yet still requires app-enablement, seatback entertainment is becoming customized to the passenger with PIN-unlock, and even boarding prioritization is unlocking ancillary revenues for the airline with boarding group verification at the gate. All of those new revenue models are built on the concept of zero trust.

**In the Satellite and Space sector, a similar revolution is underway whereby unlocking the next level of growth and capabilities will require redefining the ownership = control = security paradigm. More automation will be required which will increase the threat plane.** Data will become more sensitive requiring more sophisticated security paradigms. Auditing and analytics will be mission-critical. In short, verification throughout the owned vs. shared infrastructure network of tomorrow is required for success.

In the context of a widening and deepening attack surface in space, players across the satellite value chain must assume that attacks and breaches are inevitable, pressing for software solutions that can mitigate risks dynamically. The Zero Trust Architecture is not uniquely associated with a single product or service because ZTA is really about pursuing a comprehensive cybersecurity strategy that scales and adapts. Nevertheless, there are industry experts with products and services specifically designed to align with such strategy, addressing the satellite sector vulnerabilities and their unique interworking with other industry sectors. Solutions span from enhancing the security of embedded devices, to shifting intelligence to the edge, to fully delivering on the promise of the ZTA concepts.

> *A satellite that can survive launch and initiate operations in space is no longer the benchmark for excellence. A satellite must be capable of defending itself against all sorts of threats – with security built into every layer of operations, in space and on the ground*[10]



**Rob Spicer**
CEO, TriSept

One of such solutions is TriSept Security Enhanced Layer[10], a Linux based operating system for embedded devices, with a focus on providing a general purpose OS for satellites of all sizes. Other players like WindRiver[11] are focused on building security solutions for the "intelligent edge" with continuous development and updatability, not only to patch vulnerabilities and repair damage but also to add functionality and improvements. One company, SpiderOak, has gone beyond these solutions with its OrbitSecure Platform[12], a ZTA-based software solution specifically designed for ground and space platforms that require high security. OrbitSecure enables security when application owners

[10] https://trisept.com/trisept-security-enhanced-layer/
[11] https://www.windriver.com/solutions/aerospace-and-defense
[12] https://spideroak.com/orbitsecure/

differ from infrastructure owners by managing permissions using distributed ledger technology (blockchain).

# Business Considerations and Bottom Line

The commercial space industry is rapidly growing across multiple layers, adding new challenges to cybersecurity. While many of the challenges in space are common to those in terrestrial and wireless networks, risks in space are also quite unique. Increasing popularity in leveraging off-the-shelf components in space assets, software defined networks, and as-a-service implementations that interplay with cloud ecosystems enable new revenue sources for stakeholders, but also major cybersecurity threat vectors. As more of these revenue sources proliferate across heterogeneous networks, legacy security systems quickly become insufficient to support the best-in-class protection required to operate in dynamic, reconfigurable networks.

Lack of cybersecurity at the level required for the revenue generation potential has negative implication for business, as poor security may act as a deterrent for leveraging the abundance of innovations and assets in space networks. In this new environment with increasing dynamics, the new cybersecurity paradigm is about trusting less by adopting a resilient, Zero-Trust security framework. Under such assumptions, security breaches do not matter as much because of their contained impact as a result of the inherent mechanisms present in a self-evolving and extensible cybersecurity framework that self heals, effectively functioning like a network-level immune system.

All layers of the space sector value-chain must upgrade their cybersecurity practices across current legacy systems:

- Government and military end-users may focus significant resources on cybersecurity. A large portion of existing space-based systems have integrated cybersecurity measures, which have kept them out of the headlines. However, these measures have relied on continuous upgrades, involving significant financial or human resources. A new framework with self-evolving capabilities is needed to scale.

- Private companies dedicate their own resources to avoid cyber breaches and they are typically over-dependent on traditional cybersecurity models such as perimeter defense to ensure legacy platform compatibility. However, the push towards dynamic, multi-domain business environment with software-defined networks and cloud-empowered applications challenge the effectiveness of traditional security.

- Space startup companies must be aware of the vulnerabilities in their infrastructure while focused on building the next era of space products and services, not only to protect their own business but also to protect their customers' data and privacy. Increasingly, 'their infrastructure' does not mean 'infrastructure they own' but instead leverage services-based business models.

Zero trust therefore represents a fundamental shift from a perimeter security and location-centric trust to a software-driven approach with granular flexibility across networks, systems, data and assets with functions that change over time. While powerful, shifting to a ZTA is non-trivial, requiring need to drive implementations in partnership with industry experts. Space stakeholders can be secure -even in a hosted payload environment- by adopting the right technology that enables a robust ZTA risk management strategy.

# ABOUT NSR

## AHEAD OF THE CURVE

As the satellite & space industry boldly expands in new directions, success is directly aligned with your ability to know where the market is headed and why. NSR helps you get there first.

Founded in 2000, NSR is a global leader in Satellite & Space Market Research and Consulting Services. NSR specializes in the analysis of growth opportunities across four core industry sectors: Satellite Communications, Satellite & Space Applications, Financial Analysis and Satellite & Space Infrastructure.

The NSR team consistently forecasts events and trends well ahead of when they become common industry knowledge. Our clients get results that are broader, balanced, and with the most honest assessment of the impact to their particular business.

### NSR Contributors to this White Paper


**Brad Grady**
President & COO
bgrady@nsr.com

**Charlotte Van Camp**
Consultant
cvancamp@nsr.com

**Shivaprakash Muruganandham**
Consultant
smuruganandham@nsr.com

**Carlos Placido**
Consultant
cplacido@nsr.com