Written Testimony of Daniel Gizinski
President, Satellite & Space Segment, Comtech Telecommunications
On
Signal Under Siege: Defending America's Communications Networks
Before the
Telecommunications and Media Subcommittee
Of the
United States Senate Committee on Commerce, Science, and Transportation
December 2, 2025

Chairman Fischer, Ranking Member Luján, and Members of the Subcommittee,

Thank you for the opportunity to speak with you today. My name is Daniel Gizinski, and I serve as President of the Satellite and Space Communications (S&S) Segment at Comtech. Today, Comtech delivers resilient, high-performance satellite ground systems and secure communications technologies that enable real-time connectivity for government, defense, and commercial missions – most of which are designed, manufactured, and supported in the US. I appreciate the opportunity to contribute to this important discussion.

As this Subcommittee has recognized, America's communications infrastructure is under increasing pressure from foreign adversaries who are using advanced technologies to infiltrate, disrupt, and exploit our networks. Satellite communications are a critical part of that infrastructure. They enable everything from global military operations to emergency response and commercial connectivity. And yet, they have historically received less attention than terrestrial networks when considering cybersecurity and our national defense posture.

Since their inception, satellites have played a foundational role in global communications. Geostationary satellites (GEO) have long provided backhaul for remote cellular towers, broadcast services, and critical infrastructure links. For areas underserved by fiber or terrestrial wireless networks — remote, rural, mountainous regions, or even maritime environments — satellite links have often been the only feasible way to transport traffic.

The industry has seen tremendous innovation over the past five years, including the emergence and build-out of large-scale non-geostationary orbit (NGSO) constellations, including SpaceX's Starlink, Amazon's Leo constellation (formerly Project Kuiper), SES's O3b mPOWER network, and Eutelsat OneWeb, among many others. These systems deliver high-speed, low-latency connectivity to users around the world, including in rural and underserved areas where traditional infrastructure doesn't reach and enable new capabilities in maritime, aviation, defense, and enterprise markets.

At the same time, we're seeing the emergence of the direct-to-device market – connecting smartphones and other small devices directly to satellite with companies like Apple, AST SpaceMobile, and Lynk Global. This has the potential to transform emergency response, expand mobile coverage globally, and provide critical connectivity services in underserved locations or areas impacted by natural disasters.

What makes this moment especially important is the pace of change. Unlike traditional geostationary satellites, which typically have an operational lifecycle of 15 to 20 years, low-earth orbit (or LEO) constellations are built on much shorter technology cycles, typically 5 to 7 years. That means the industry is evolving quickly, with new capabilities and risks emerging constantly. Our regulatory and security frameworks need to keep up.

At the same time, the threat landscape is becoming more complex. Satellite networks naturally present a broader attack surface than terrestrial systems – many of the satellites providing coverage to the United States expose network traffic outside of our borders.

Yet many of the cybersecurity practices in the sector haven't kept pace. A recent study by researchers at the University of California, San Diego, and the University of Maryland[1], showed that a significant number of geostationary satellite signals are still being transmitted without encryption. Using an $800 off-the-shelf receiver and a rooftop dish, the researchers were able to intercept sensitive data from commercial airlines, cellular networks, critical infrastructure, and even military and law enforcement communications.

This wasn't a sophisticated cyberattack. It was a clear example of how basic security practices like encryption are still not universally applied, even when called for by existing security frameworks.

Additional research has revealed vulnerabilities in commercial satellite modems, including insecure firmware update paths, exposed web interfaces, and outdated protocols. In a number of instances, encryption was disabled by default.[2] A number of other attack methods have been demonstrated against a variety of satellite systems.[3] One of the potential reasons this has not been more readily explored is there is little reward to attract low-level cyber criminals to satellite systems – in contrast, there is substantial interest to nation-state actors. Our security posture must recognize the level of sophisticated threat actors these systems face.

Five main threat actors and advanced persistent threat (APT) groups have targeted satellite communications technology, with others having conducted attacks as well (Flashpoint, 2024). These attacks include exploiting legacy protocols, insecure firmware, and unpatched systems to gain access to sensitive data and disrupt operations.

We strongly encourage a thoughtful approach to securing these critical systems. Satellite communications provide a lifeline for both defense and commercial users. Today, satellites enable global command and control, real-time intelligence sharing, logistics coordination, and resilient communications in denied or degraded environments. Enterprises rely on satellite networks for everything from maritime and aviation connectivity to oil and gas operations, disaster response, and financial transactions. A successful cyberattack on a commercial satellite link or gateway could disrupt services across continents, compromise customer data, or even impact national

[1] Don't Look Up: There Are Sensitive Internal Links in the Clear on GEO Satellites
[2] A Comprehensive Analysis of Security Vulnerabilities and Attacks in Satellite Modems
[3] PowerPoint Presentation

economies. At the same time, many of these systems are highly complex, expensive, and take a significant amount of time to deploy, which may limit the pace at which new defensive capabilities can be reasonably fielded. Satellite systems are exposed to risks across their space segment, user segment, link segment, and ground segment – each with unique considerations and complexities.[4]

In the case of the space segment – components are typically not accessible following launch, which limits the ability to field certain updates. There are simple fixes available for certain use cases – what I refer to as common-sense cyber hygiene. Enabling encryption, either on the satellite modem or in-line, is a low cost and simple step, and one we recommend to our customers – as do many of the existing satellite security compliance frameworks.[5] Despite many frameworks calling for encryption on satellite links, we still see networks operated without this protection step in place.

Rigid, rules-based frameworks often rely on static checklists and controls that have been written and developed in response to past incidents, rather than in anticipation of future threats. Flexible frameworks that promote collaboration between industry and Government, encourage thoughtful risk-based decision-making, and enable flexibility will be key to developing a culture of innovation around cybersecurity. This cultural shift will be key to promoting innovation in security that keeps pace with commercial innovation.

Strong cyber posture can be built effectively with a framework that brings together government and industry to share threat intelligence, aligns incentives, and responds quickly to emerging risks. Protection requirements should be aligned with risk, understanding that not all data requires the same treatment. Our adversaries are looking forward in their approach to developing attacks, and our defense posture should reflect that.

First, information sharing at the speed of relevance is critical, and a point that has broad support across the industry. The Satellite Industry Association (SIA) is a US-based trade association that provides representation of leading domestic satellite operators, service providers, manufacturers, and more.[6] SIA has long emphasized that cybersecurity is central to the satellite industry's mission of providing secure, reliable, and resilient connectivity. SIA also highlights the importance of voluntary information sharing. Sector participants often face common threats, and they must be free to collaborate among themselves and with government to identify and respond to attacks, share mitigations, and learn from past experiences. Information sharing benefits should be secure, confidential, and free from fear of liability or regulatory consequences. This principle is essential to building trust and strengthening the entire ecosystem. Ensuring that this collaboration includes both industry and government perspectives is critical in an era where sophisticated attacks are common.

Second, I believe we should consider how to move beyond compliance-only frameworks and begin incorporating incentive-based models into our cybersecurity posture. Today, much of the

[4] Recommendations to Space System Operators for Improving Cybersecurity
[5] Security and Privacy Controls for Information Systems and Organizations
Introduction to Cybersecurity for Commercial Satellite Operations
[6] About Satellite Industry Association (SIA) – Washington, DC

focus is on penalties for breaches or non-compliance. But there's also an opportunity to reward forward-looking behavior and encourage industry to bring innovative approaches forward. Organizations that invest in proactive security measures, adopt modern encryption standards, or participate in collaborative threat-sharing initiatives could benefit from things like tax credits, grants, or streamlined certification processes. Cybersecurity tends to operate as a cost-center in most organizations, and an incentive program would help industry thoughtfully allocate both effort and talent. These are ideas worth exploring as part of a balanced and practical approach to security.

Third, we need to recognize that cybersecurity can't be an afterthought. It has to be built in from the start, across all layers of a system. That means designing subcomponents with security in mind: secure boot, memory-safe programming languages, authenticated firmware updates, and architectural decisions that prioritize security alongside performance and cost[7]. This means extending threat sharing beyond service providers to many levels of the supply chain, ensuring that all layers of the tech stack are designed with security in mind. Supply chain security remains a critical component, and ensuring that appropriate attention is paid to both the origin of hardware and software is key[8].

There's also a growing gap between the people writing cybersecurity policy and the people building the systems. We're seeing more professionals enter the field who understand the security rules but may not fully understand the full architecture, product technology, ecosystem, and/or the potential threat landscape. We need to make sure cybersecurity expertise is integrated into system design from the beginning, not added on later.

With the exponential growth and technology trajectories of this sector and satellite connectivity becoming increasingly interwoven into the daily fabric of our lives and our nation's security, it's clear that satellite communications must be treated as a priority within our national communications infrastructure. Satellite connectivity currently supports a wide range of critical daily services, it is playing a central role in helping expand connectivity access to underserved communities, it is a key enabler of defense and emergency response operations, and satellite connectivity is continuing to drive innovation across industries. The cyber threats this sector faces are real, and they are evolving quickly. If we want to ensure the long-term resilience and security of this sector, we need to give it the attention it deserves and be willing to rethink how we approach oversight, collaboration, and innovation.

I appreciate the opportunity to appear before you today on behalf of the satellite industry and I am happy to answer any questions.

[7] Cybersecurity in the Space Domain: Why It’s Time to Stop Leaving the Front Door Unlocked - Comtech Telecommunications Corp.
[8] Comtech-WP-Ground-Station-Cyber-Threats-and-Product-Design-Techniques-for-Defense.pdf