NATIONAL SECURITY SPACE ASSOCIATION

NATIONAL SECURITY SPACE ASSOCIATION
MOORMAN CENTER FOR SPACE STUDIES

Keynote speech given to a roundtable on

Cybersecurity and Resilience of Satellite Systems

at the Embassy of the Czech Republic, Washington, DC
by Dr. Scott Pace

January 12, 2026

In the 1920s and 30s, as aviation grew in global importance for military and commercial needs, Czechoslovakia was an enthusiastic pioneer. “The air is our sea” was a phrase that captured the hopes and ambitions for a newly independent, but land-locked country.

Today, space is the new ocean which links all nations for science, commerce, and conflict. As President Kennedy said at the opening of the space age, humanity will decide whether this new ocean will be “a sea of peace or a new terrifying theater of war.” If you look up at the night sky, you know it is not empty. Thousands of satellites orbit overhead, providing global communications, navigation signals, precision time, and virtually continuous images of the planet.

Space capabilities are fundamental to multiple critical infrastructures essential to the global economy and which provide for public safety and national security. The power of space systems comes not from rockets and satellites themselves, but the information that flows up, across, and down from space and into our critical infrastructures. Space power is about the power of information. Thus the security of space is integrally tied to the cybersecurity of space systems and the security of globally connected systems that they touch.

Space represents yet another evolving aspect of the information revolution of recent decades. Unlike Cold War competition, space is not the exclusive domain of super powers. Space is increasingly democratized and globalized, with new stakeholders of all sizes seeking new opportunities. As a result of globally connected systems, space cybersecurity is not just a concern of satellite operators. Success or failure touches everyone, whether or not they are even aware of their reliance on space.

Cyber Threats to Space Systems

Cyberattacks on space systems are not new. NASA and ESA have experienced multiple incidents over the years as global connectivity and international cooperation have grown. A watershed moment in global public awareness of space cyberattacks was the 2022 Russian cyberattack on Viasat’s GEO satellite broadband service, just prior to the invasion of Ukraine. The attack disrupted internet service for tens of thousands of users in Ukraine and Europe, causing communication losses for Ukrainian forces and collateral damage to energy systems in German and France. The attack gained access to ground network management systems, exploited a VPN misconfiguration, and remotely wiped modems using “AcidRain” malware.

In contrast, Russian cyberattacks on Starlink have been largely ineffective due to a combination of SpaceX’s ability to rapidly deploy software updates, the system’s inherent physical characteristics, and the distributed nature of the satellite constellation. When Russia attempts a cyberattack or jamming, Starlink’s engineering team can quickly patch vulnerabilities and mitigate the attack, often within a day. This speed of response has been described as “eye-watering” by U.S. defense officials. Furthermore, the data transmitted over the network is encrypted, and Starlink antennas use narrow beams in the Ku and Ka frequency bands. An attacker attempting to jam the signal needs precise aim and must be in close proximity to the user terminals, making physical attacks difficult to execute effectively over a wide area. Starlink’s large constellation of thousands of satellites means that taking out a single satellite or ground station achieves little, as the network can reroute traffic.

The primary cyber threats to space systems—particularly commercial satellites—revolve around vulnerabilities in ground infrastructure, TT&C links lacking encryption, onboard software, and human factors. These threats exploit the increasing reliance on commercial components, global supply chains, and legacy systems, potentially leading to loss of satellite control and disruptions in services like navigation, communications, and broadband internet.

Communications Protocol Compromise via Social Engineering

Attackers use tactics like spear-phishing to gain access to ground control centers, then laterally move to hijack protocols between mission control, ground stations, and satellites. This enables eavesdropping, command alteration, or full takeover, potentially crashing satellites or broadcasting malicious signals. Insider threats, inadequate employee training and poor network segmentation can make social engineering attacks relatively cheap.

Network Intrusion from Misconfigurations and Weak Security Protocols

Attackers can exploit open ports, unpatched ground station networks, and a lack of encryption in gateways or control systems. This allows persistent access for data exfiltration, ransomware, or denial-of-service attacks that propagate to users. One way this can occur when satellite terminals are rushed into service in response to natural disasters or other emergencies or, less excusably, when operators fail to follow standard precautions and authoritative advisories on cybersecurity.

Exploiting Onboard Computer/Software Vulnerabilities via Malicious Code Injection

Malicious code can be inserted into satellite onboard computers or software during manufacturing, supply chain transport, or firmware updates, exploiting unpatched commercial components. Once in orbit, it can execute unauthorized commands, corrupt telemetry, or cause orbital maneuvers, leading to loss of satellite control. These kinds of attacks are more sophisticated and expensive, but effective against space systems that fail to explicitly defend against them.

While electronic warfare remains a concern (e.g., GPS jamming and spoofing in conflict zones and Russia's disruptions in the Baltic Sea region), purely cyber risks are escalating with the growth of commercial space services. These threats highlight the need for cybersecurity-by-design principles, such as supply chain vetting, regular patching, and employee training.

Unique Challenges for Space Cybersecurity

Many satellites currently in orbit were designed to survive in a hostile physical environment —not ransomware, firmware tampering, or state-sponsored cyber-espionage. Legacy inertia is a cybersecurity vulnerability. A modern terrestrial cybersecurity strategy is known as Zero Trust. As described by NIST (the National Institute of Standards and Technology), Zero Trust requires continuous authentication, authorization, and least privilege access for every request to resources, treating all traffic as potentially hostile. It's "never trust, always verify" using techniques like multi-factor authentication (e.g., when you receive a pass code on your cell phone), micro-segmentation of software tasks, and continuous monitoring.

Implementing Zero Trust in space systems presents unique challenges beyond typical enterprise environments, primarily due to resource constraints, intermittent connectivity, reliance on legacy systems, and the physical inaccessibility of assets in orbit.

- **Resource and Environmental Constraints:** Space systems operate under strict limitations regarding computational processing power, memory, size, weight, and power (SWaP). This makes it difficult to conduct frequent updates, or implement resource-intensive cryptographic solutions needed for continuous authentication and monitoring.
- **Intermittent Connectivity and Latency:** Satellites often have limited or delayed connectivity with ground stations, affecting the latency of ground-based services and real-time monitoring. This lack of consistent, high-bandwidth communication makes continuous verification highly challenging in practice.

- **Legacy Systems Integration:** Many space assets currently in orbit were designed with perimeter-based security models and often run on aging hardware and software. Integrating these legacy systems into a zero-trust framework without creating security gaps or requiring a complete, costly replacement is a major hurdle.
- **Limited Incident Response and Monitoring:** If an attack occurs in space, the ability to respond is significantly limited by distance, bandwidth constraints, and the inability to perform on-site physical maintenance or quick patching.
- **Need for Autonomy:** The significant latency in space communication means that systems must be able to operate autonomously in a trustworthy manner without constant human input or ground-based verification. Developing systems that can make independent, trusted security decisions is an on-going area of research.
- **Physical and Supply Chain Risks:** Space systems are vulnerable to physical attacks like signal jamming and spoofing, which don't require direct access to the satellites themselves. International supply chains for commercial components also introduces risks, as compromised components or software could be integrated before launch.

At present, legacy hardware deployed in orbit often lacks the technical capacity to support regular software updates or the implementation of newly developed security mechanisms, thereby significantly constraining the long-term cybersecurity resilience of space systems. Cyber resilience in space needs to move as fast, if not faster than the rest of the space sector.

Pillars for a Secure Space Future

The International Telecommunication Union (ITU) coordinates global telecommunications standards, manages radio-frequency spectrum, and promotes equitable access to information and communication technologies (ICTs), which includes space systems. Space cybersecurity—encompassing the protection of satellites, ground stations, launch systems, and related networks from cyber threats such as hacking, jamming, spoofing, and signal interference—is a critical extension of the ITU's mandate.

The Global Cybersecurity Forum is a non-profit, NGO based in Saudi Arabia. In cooperation with the ITU, they have a Global Cybersecurity Agenda based on five pillars: legal measures, technical measures, organizational measures, capacity building and international cooperation. Since this is a conference about cybersecurity regulation, let me briefly address legal measures.

My university recently had the pleasure of hosting Anna Blechová from the Czech Republic as a visiting scholar. One of her observations is that the regulatory landscape is characterized by a significant tension between hard law (binding treaties and national legislation) and soft law (non-binding guidelines, standards, and best practices). While hard law provides authority and liability frameworks, it is often criticized for being outdated and slow to evolve; conversely, soft law offers flexibility and technical precision but frequently lacks the enforceability needed to motivate industry-wide investment.

Existing international law is often described as insufficient and ambiguous regarding cyber-specific threats. In a partial response, the European Union is seeking to create new hard law. The NIS 2 Directive classifies ground-based space infrastructure as high-criticality, though its scope is largely limited to terrestrial assets. To bridge this gap, the European Commission's draft EU Space Act (2025) aims to introduce binding cyber-resilience obligations for both on-orbit and ground infrastructure, including mandates for risk assessments, encryption, and incident reporting. In the United States, Executive Order 14144 (2025) directs updates to federal acquisition regulations to require risk-based, tiered cybersecurity capabilities for civil space systems.

Soft law such as international standards from organizations like ISO and IEEE, as well as multi-agency and agency-specific policies from NIST and NASA, has become a primary mechanism for addressing technical challenges. Soft law based on transparent, technically-grounded "open standards openly arrived at" is often easier to create and find consensus on among international partners and private entities. Soft law should be taken seriously as it has the potential to evolve into hard law over time through international custom or by being integrated into legislation.

Hard and soft laws are vital tools and platforms for sharing ideas and best practices, but we should be wary of thinking that legal measures alone are a solution. Criminals and rogue states will not care about legal measures, of course. We need the other pillars of technical measures, organizations, capacity building and international cooperation.

Shared Responsibilities

Cyber threats do not respect borders. Defeating those threats requires multi-stakeholder dialogue, leveraging partnerships between governments, the private sector, and academia. Space cybersecurity should no longer be viewed as a "bolt-on" feature or a constraint on innovation, but as a foundational requirement for mission success.

We need to expand sharing of real-time threat intelligence and best practices, at least among likeminded countries and the private sector. To this end, I hope the Czech Republic will be working closely with NATO allies, in particularly noting the work being done by Estonia.

There is a critical shortage of professionals with expertise at the intersection of aerospace and computer engineering. We need to invest in interdisciplinary training and human capital to bridge the cultural gap between satellite engineers and cyber analysts.

Least Developed Countries (LDCs) and Small Island Developing States (SIDS) rely heavily on satellites to overcome terrestrial infrastructure gaps. However, these nations often lack the technical expertise and resources to secure these vital links. International cooperation should include capacity-building seminars and affordable toolsets to ensure that every nation can operate securely in space.

Let us commit to looking up, not with complacency or ignorance, but with the vigilance and cooperation required to ensure that space remains a secure, productive, and peaceful frontier for all of humanity.

Dr. Scott Pace presented this paper at the Embassy of the Czech Republic in Washington, D.C., on January 12, 2026. Dr. Pace is the Director of the Space Policy Institute and a Professor of the Practice of International Affairs at George Washington University's Elliott School of International Affairs.

The views expressed herein are solely those of the author and do not reflect the views of the Association or its member companies.

NSSA is the only U.S. trade association dedicated solely to promoting the health and vitality of the U.S. national security space enterprise (Title 10 and Title 50) and its supporting industry partners. For more information, including how to join the Association, please visit us at www.nssaspace.org.