

Strengthening Space Resilience, Creating Dependencies

Dr. Sarah McKee (CNTR/PRIF)

It is no surprise that space has become increasingly integrated into national security, economic activity, and critical infrastructure. Day-to-day activities such as ride-sharing, weather forecasts, online banking, and more complex services like robotic surgery, water purification, and precision agriculture all rely upon space products and services, which underpin the operation and resilience of multiple critical infrastructure sectors. As competition over scarce space resources increases, Western governments and commercial operators have increasingly focused on **resilience** through:

Larger satellite
constellations

Distributed
architectures

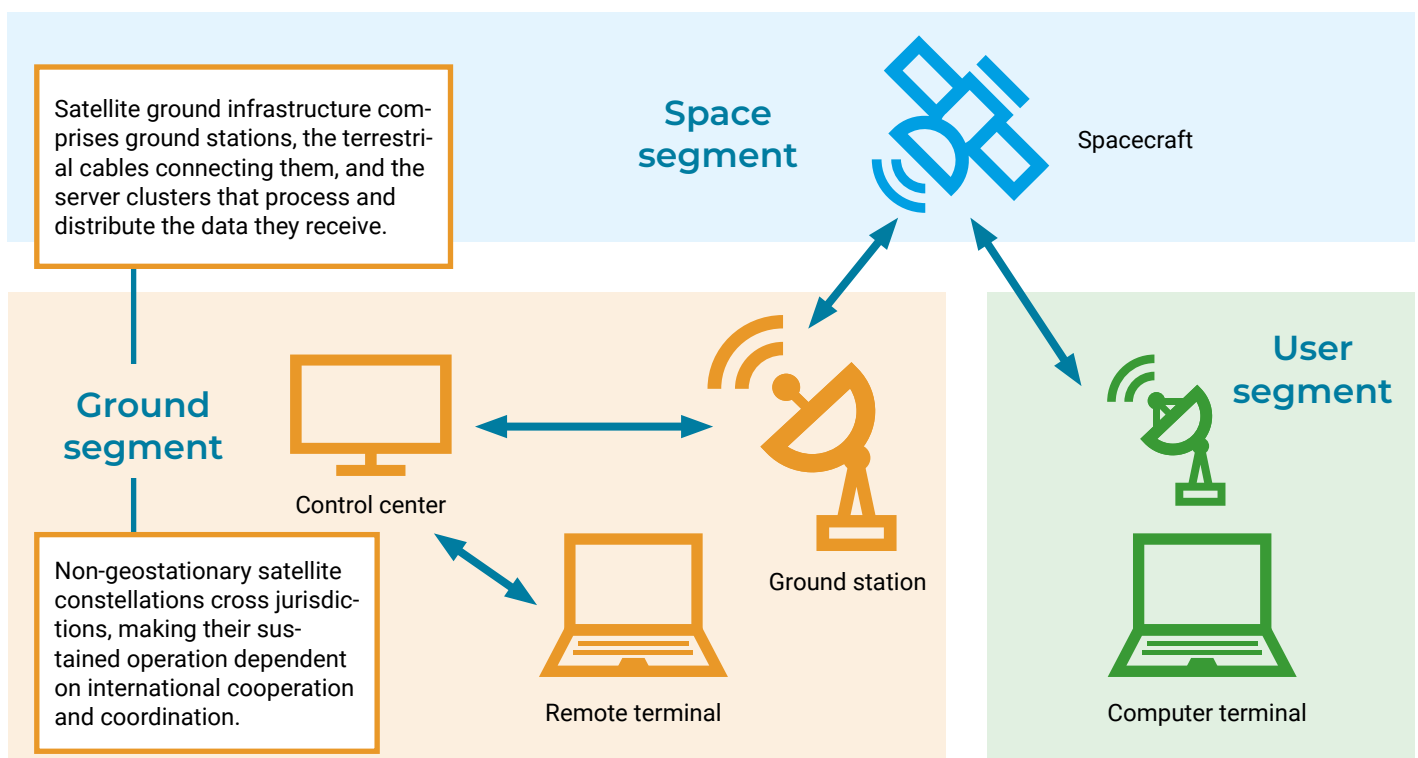
Commercial
augmentation

Rapid replacement
capabilities

Redundant orbital
systems

Resilience, however, should not be measured solely by the number of satellites in orbit. The security strategy behind resilience by proliferated constellations, attempts to achieve deterrence by denial, such that with larger numbers of satellites across multiple orbital planes, it would be more difficult for an adversary to eliminate space-based capabilities through direct attacks on individual spacecraft. However, this approach underestimates a known vulnerability: satellites do not yet operate fully autonomously. Space capabilities depend on a terrestrial ecosystem of ground stations, communications networks, data processing centers, and skilled operators.

Ground stations communicate with satellites, send commands to them, and receive the data they transmit back to Earth. **Control centers** are operational hubs where teams of operators monitor satellite health and manage their activities and movements in orbit.



Space systems function as interconnected segments that collectively provide data and services to end users. Compromise of any one segment can disrupt the end-to-end transmission of information to users.

ASAT vs Counterspace Operations

Although anti-satellite (ASAT) weapons dominate discussions of space conflict, they represent only one subset of counterspace operations. Many counterspace activities are directed not at satellites in orbit, but at the ground infrastructure, communications networks, and data systems that underpin space capabilities. In practice, the first shots of a space conflict may be fired on Earth rather than in orbit.

Counterspace Operations

As per the UNIDIR Space Security Lexicon, counterspace operations are capabilities, techniques, or assets that can be used against another space object or a component of a space system in order to deliberately deny, disrupt, degrade, damage or destroy it reversibly or irreversibly, so as to gain advantage over an adversary.

Moving beyond an anti-satellite (ASAT)-centric view, an adversary does not necessarily need to destroy satellites to defeat a space-enabled capability. Given that space systems rely on both space and ground segments, **attacks against terrestrial infrastructure may be sufficient to disrupt, degrade, or deny space-enabled services even while the satellites themselves remain operational.** This broader understanding of counterspace operations also raises questions about the relationship between space systems and critical infrastructure. Commercial satellite networks increasingly support essential services and military operations alike, creating ambiguity over whether such systems should be regarded primarily as commercial infrastructure, critical infrastructure, or military enablers.

This tension is illustrated by recent Iranian claims regarding Starlink. Following allegations that Starlink had supported attacks against Iranian critical infrastructure (water infrastructure reportedly), Iranian authorities reportedly identified Starlink ground stations and other SpaceX infrastructure in the region as legitimate targets. Regardless of the validity of these claims, the episode illustrates a reciprocal dynamic: space-enabled systems may be perceived as supporting attacks against critical infrastructure, while the space infrastructure itself may subsequently be treated as a critical target.

Illustrative space-enabled critical infrastructure sectors



Water management & purification



Transportation & logistics



Energy generation & distribution



Precision agriculture & food production



Communications & navigation

Policy Debate: Space Systems as Critical Infrastructure

Critical Infrastructure are those assets, systems, and networks performing functions considered to be critical to the functioning of a society. Space systems can themselves be considered critical infrastructure but also sub-systems of critical infrastructure in other sectors, depending on the specific technology. The EU recognizes space as a critical sector within legislation on the resilience of critical entities (CER Directive) and cybersecurity (NIS2 Directive). The ground infrastructure of Member States and private operators, as well as satellites used for delivering telecommunication services, are considered as part of critical digital infrastructure. However, the translation of this EU-level recognition into national critical infrastructure frameworks remains uneven. Germany's proposal to establish a dedicated critical infrastructure sector for space reflects the ongoing evolution of national policies in this area.



Key observations

- The ability of satellites to survive an attack is not the same as the ability of a space system to continue providing services.
- Ground infrastructure represents the critical interface between space assets and terrestrial users.

Appendix



Imprint

CNTR is a research alliance between the Peace Research Institute Frankfurt (PRIF), Justus Liebig University Giessen and the Technical University of Darmstadt. www.cntrarmscontrol.org
· V.i.S.d.P.: Elisabeth Waczek (PRIF), Darmstädter Landstr. 112, Frankfurt a.M., Germany, Phone (069) 959104-0, info@prif.org, www.prif.org · Design: media | machine GmbH · Layout: CNTR



TECHNISCHE
UNIVERSITÄT
DARMSTADT



Gefördert durch:



Auswärtiges Amt