Advancing Low Earth Orbit Satellite Internet Infrastructure:

Insights from the Trusted Internet Summer School on Internet Governance and International Law

Authors: Berna Akcali Gur, Jason Bonsall, Dmitry Epstein, Jung Seob (Scott) Kim, Magdalena Krysiak, Joanna Kulesza, Liljana Pecova-Ilieska, Maciek Piasecki, Célestine R. Rabouam, Roxana Radu, Monika Stachoń, Isti Marta Sukma, Liya Wang, Dan York

Łódź, 2025

Note: This document presents the recommendations from the Trusted Internet Summer School on Internet Governance and International Law, an initiative under the research project "Satellite Internet: Trust and Data Governance" supported by the Internet Society Foundation

Preamble

Low Earth Orbit (LEO) satellite broadband is a significant development in global internet infrastructure, presenting both opportunities to advance the Sustainable Development Goals and challenges related to cost, deployment, and regulation. These systems are governed by a combination of national laws and international treaties on telecommunications, trade, and outer space. As we stand at a critical juncture in the progression and adoption of this technology, it is imperative to ensure that the regulatory framework is adapted to harness the benefits of LEO satellite broadband while addressing its associated challenges. It is essential to acknowledge that the interests and priorities of underserved regions, which depend on overseas providers and stand to gain the most, will differ significantly from those on the other side of the digital divide, some of whom possess control and ownership of this type of infrastructure. Addressing this disparity is crucial for achieving fair and equitable global connectivity.

Governments have the mandate and obligation to ensure that telecommunication infrastructures operate securely and with respect to human rights, particularly preventing unauthorized access to sensitive data. This encompasses assessing the regulatory regime including cybersecurity, data privacy protection with respect to the satellite broadband specific risks. Robust regulatory frameworks are essential for safeguarding these infrastructures and the data flows they enable.

A balanced policy approach that considers both benefits and risks is essential for the sustainable development of satellite broadband. Equitable and sustainable internet access for all can only be achieved through advocacy and active engagement with local stakeholders, international bodies such as the International Telecommunication Union (ITU), the World Trade Organization (WTO), and the Committee on the Peaceful Uses of Outer Space (COPUOS), as well as the entire internet ecosystem which also includes non-governmental stakeholders. Such cooperation is necessary to guide discussions and shape a fair and inclusive internet.

Active participation in these international platforms will enable stakeholders to represent their interests and mitigate the adverse implications of deepening digital global divide. Equitable participation in these platforms is critical for addressing the digital divide and ensuring that all countries have a voice in shaping the future of internet connectivity.

Trusted Internet Summer School on Internet Governance and International Law is a part of a research project "Satellite Internet: Trust and Data Governance" supported by the Internet Society Foundation

As the number of people relying on LEO satellite broadband systems grows, it is important to enhance the resilience of these networks and the transparency of their operations. It is recommended to establish international platforms identifying and addressing vulnerabilities within these systems, including through security assessments where authorized individuals simulate cyberattacks on a system to identify and exploit vulnerabilities to reinforce resilience and confidence in the technology.

In the lead-up to the 20th annual review of the World Summit on Information Society, we recommend considering the following key points in relation to satellite connectivity**:**

1. Technological Challenges and Economic Opportunities

Investing in infrastructure such as local Internet Exchange Points (IXPs) can improve the resilience and latency of satellite networks and ensure better interconnection with terrestrial networks through redundancy systems and rapid recovery capabilities. Promoting interoperability is also crucial for optimizing exchanges between different systems and networks. Developing and promoting technical standards that allow interoperability between different satellite constellations and between satellites and terrestrial infrastructures is essential. Implementing these measures would ensure the continuity of services in the event of major disruptions.

The high entry costs of satellite broadband can result in an oligopolistic market. Sustainable business models must be explored to ensure broad access. The current system governed by the ITU for satellite constellations deployed in LEO, operates on a neutral "first come, first serve" approach. However, the saturation of this limited resource with satellites from a few entities could restrict access for new entrants.

2. Trust and Transparency

The Internet, initially characterized by its decentralized structure, is increasingly seeing its key aspects fall under the control of a few public and private stakeholders. Currently, this challenge is particularly pronounced in the case of satellite broadband, where competition is currently limited.

To prevent dependence risks arising from power concentration, it is imperative that public authorities are informed of the risks associated with this technology in the early stages of technology adoption. Both private and public sectors should develop expertise, engage in a robust consultation process to address concerns and demand transparency, requiring

collaboration with providers.

To enhance user and public sector confidence, it is recommended that satellite broadband operators develop mechanisms for transparency and accountability, such as publication of quarterly reports detailing their connectivity-related performance, technical incidents and security measures. Implementing annual audits conducted by independent bodies can ensure compliance with transparency regulations and security standards. These measures would strengthen operator accountability and public oversight of space activities, enabling ongoing evaluation of operator performance and compliance.

3. Environmental Concerns

Given the rising density of satellites and space debris in the LEO, mitigating significant risks to operational safety and long-term sustainability is in the interest of governments, as they are internationally accountable for operations of their private operators. Strict adherence to existing treaties and guidelines, such as the Guidelines for the Long-term Sustainability of Outer Space Activities and the Space Debris Mitigation Guidelines of the United Nations, should be mandatory. Governments must enforce these guidelines uniformly to eliminate inconsistent application. Compliance with international standards is critical to ensure that a balance is achieved between space sustainability and global connectivity goals. As this sector becomes more commercialized, all legal aspects, including intellectual property and liability to be addressed through clear legal standards and cooperative international frameworks to ensure the responsible and equitable harnessing of its benefits.

A globally adopted and enforced international regulatory framework and standards are necessary. National governments must ensure strict compliance during the pre-launch, in-orbit, and end-of-life phases of activities in the LEO. Rigorous enforcement of these standards is required to maintain order and safety in LEO. Governments should be required present proof of concept for liability measures aimed at reducing debris generation and promoting the sustainable usage of LEOs. Proactive measures and fostering international cooperation are essential to safeguard the future of space operations in LEOs. Failure to comply with these requirements will result in specified consequences as determined by the international community.

4. Workforce Development

Addressing workforce development at a strategic level is crucial for ensuring LEO satellite broadband services are used effectively and efficiently serving each region's needs. Governments must prioritize the cultivation of expertise to navigate the complexities of space technologies. This involves developing comprehensive policies and frameworks that address current and future workforce needs, ensuring strategies are in place to foster innovation, competitiveness, and economic growth in the telecommunications and space sectors.

To support the labor force layer effectively, governments need to invest in comprehensive sector-specific workforce development programs across various industries. These initiatives should focus on enhancing skills, providing continued education for experts, and promoting academic learning. This strategy ensures that the workforce remains adaptable and capable of meeting the evolving demands of the global Internet infrastructure, including the space-based segment. Initiatives should bridge the gap between academic institutions and industry, facilitating the sharing of talent and practical experience.

5. Security and Privacy

A comprehensive approach to securing LEO satellite systems necessitate coordinated action across international, national, industrial, and societal levels. The security and privacy challenges in this domain include a range of threats—such as signal jamming, kinetic attacks, electromagnetic interference (EMI), and cyber intrusions—which give rise to significant risks, understood here as the potential for damage, disruption, or unauthorized data access resulting from these threats. These are referred to as "traditional" cybersecurity threats based on established threat typologies used in terrestrial systems, such as the MITRE ATT&CK framework and ENISA threat taxonomy, but increasingly applied to the space domain.

For instance, signal interference undermines operational continuity, data integrity, and communication reliability. Physical threats—including kinetic destruction by anti-satellite weapons—generate space debris and compound collision risks. EMI disrupts navigation and communication systems, affecting both security and data confidentiality. Cyberthreats such as malware, unauthorized access, eavesdropping, or ransomware attacks can exploit system vulnerabilities, compromising both user privacy and system functionality.

To mitigate these risks, actors must adopt robust cybersecurity frameworks that integrate encryption, multi-factor authentication, continuous monitoring, and resilience mechanisms. Applying privacy-by-design and security-by-design principles is essential, ensuring that

privacy and data protection norms are embedded in the development and deployment of satellite technologies. Organizational resilience should also include contingency planning, red-teaming, and capacity-building through regular employee training.

Given the implications for human rights, data privacy, and global communications, governance efforts should include inclusive, multistakeholder engagement. This includes developing international standards for LEO satellite security, supporting research into protective technologies, and establishing regulatory and cooperative frameworks that enable information exchange and harmonized best practices. The role of civil society, industry, academia, and states is indispensable in shaping a rights-respecting, secure space environment.

6. Social and Political Considerations

The potential for LEO satellite broadband to rectify existing inequalities must be addressed, ensuring it remains affordable for those who need it most. Ownership of infrastructure should not amplify global mistrust but rather promote equitable access and trust among all nations.

Key Policy Questions for LEO Satellite Broadband Governance

1. **Regulatory Control and Sovereignty**
    - *What international legal or institutional mechanisms can be strengthened or established to prevent private satellite broadband providers—and their host states—from exercising disproportionate or unregulated influence over internet access and connectivity in foreign jurisdictions?*
    - *How can global governance structures ensure the equitable distribution of orbital and frequency resources to prevent infrastructure-driven digital hegemony?*
2. **Technological Feasibility and Infrastructure Centralization**
    - *To what extent do emerging inter-satellite communication technologies enable the operation of global satellite constellations with minimal reliance on geographically distributed ground stations?*
    - *What are the geopolitical and sovereignty implications of technical architectures that allow centralized control of connectivity from a single territory or limited jurisdictions?*
3. **Human Rights and Ethical Implications**
    - *What potential risks do LEO satellite broadband systems pose to fundamental rights, including privacy, freedom of expression, and access to information—particularly in conflict zones, authoritarian regimes, or marginalized communities?*
    - *What legal, institutional, and technical safeguards should be mandated to ensure that the deployment and operation of LEO systems adhere to international human rights standards, including transparency, accountability, and due process protections?*

Trusted Internet Summer School on Internet Governance and International Law is a part of a research project "Satellite Internet: Trust and Data Governance" supported by the Internet Society Foundation

Further Considerations

We must ensure that the resources associated with LEO satellite broadband are allocated for the benefit of all humankind, rather than individual companies or states. The varying capabilities of countries in technology development increase their dependence on developed countries, which can distance the UN from its sustainable development goals.

LEO connectivity can provide reliable communication to people in remote areas or regions affected by disasters, including civil society organizations (CSOs), journalists, and whistleblowers. It is crucial that economic barriers or fear do not hinder this access for anyone who wants to contribute to society. Making this technology more widely accessible can help obscure the data of CSOs, enabling them to blend in with the crowd.

We need to ensure the highest standards of encryption and company transparency, discouraging black-box approaches. There are potential trade-offs where less-resourced countries may need to provide data or other concessions to access technology and support from more developed nations or their private sectors. This dynamic can lead to a form of digital colonialism, where data from these regions is extracted and monetized by foreign entities, undermining the sovereignty of less-resourced nations. It can also result in unequal partnerships with terms heavily skewed in favor of more technologically advanced countries.

Trusted Internet Summer School on Internet Governance and International Law is a part of a research project "Satellite Internet: Trust and Data Governance" supported by the Internet Society Foundation

Internet Society Foundation

Policy Cheat Sheet: LEO Satellites and WSIS Recommendations

1. Capitalize on LEO Opportunities

- **Governmental Action**: Harness LEO satellite broadband to bridge connectivity gaps while preventing a technological hegemony dominated by a few actors.
- **Regulatory Frameworks**: Strengthen national expertise in space law, cybersecurity, and data governance to effectively manage and safeguard its interests from risks associated with the use of this emerging infrastructure.

2. Balanced Policy Approach

- **Policymaker Engagement**: Promote multi-forum dialogue (e.g., IGF, ITU, WTO, COPUOS) to shape equitable and sustainable digital futures.
- **Global Participation**: Ensure inclusive international engagement to mitigate the digital divide and foster cooperative governance.

3. Transparency and Standards

- **Early Public Involvement**: Mandate early-stage consultation with stakeholders to curb monopolistic control and enhance oversight.
- **Interoperability**: Promote interoperable technical standards and transparent data-sharing mechanisms between satellite and terrestrial systems.

4. Support Open Internet Standards

- **Standard Advocacy**: Endorse open, secure, and interoperable internet standards to preserve an open digital ecosystem.
- **Data Privacy**: Uphold end-to-end encryption and user confidentiality in LEO network transmissions.

5. Promote Localized Infrastructures

- **Local IXPs**: Invest in local Internet Exchange Points to reduce latency and improve network resilience.
- **Shared Assets**: Encourage shared ground infrastructure to reduce costs and ensure redundancy.

6. Implement Security Measures

Trusted Internet Summer School on Internet Governance and International Law is a part of a research project "Satellite Internet: Trust and Data Governance" supported by the Internet Society Foundation

- **Robust Security**: Apply defense-in-depth strategies, including secure design, monitoring, and encryption.
- **Threat Mitigation**: Address traditional and emerging threats (e.g., EMI, cyber intrusions, kinetic attacks) through international cooperation and technical safeguards.

7. Economic Considerations

- **Anti-Monopoly Regulation**: Prevent market capture by dominant actors; enable new entrants and fair competition.
- **Sustainable Models**: Develop inclusive business models ensuring affordability and viability across socio-economic contexts.

8. Legal Frameworks

- **International Compliance**: Adhere to the Outer Space Treaty, Guidelines for the Long-term Sustainability of Outer Space Activities and UN Space Debris Mitigation Guidelines; enforce uniform application.
- **Jurisdictional Clarity**: Establish legal certainty for cross-border operations and liability in satellite governance.

9. Workforce Development

- **Talent Investment**: Support space-sector education, continuous training, and multidisciplinary programs.
- **Academic-Industry Collaboration**: Facilitate partnerships to ensure practical skill development and innovation exchange.

10. Security and Privacy

- **Cyber Policy**: Embed privacy-by-design and security-by-design principles; enforce continuous auditing and risk mitigation.
- **Operational Resilience**: Implement contingency planning, red-teaming, and regular drills to ensure preparedness.

11. Social and Political Considerations

- **Equity Focus**: Ensure affordable access, especially for marginalized and disaster-affected communities.
- **Prevent Digital Colonialism**: Guard against extractive data practices; uphold sovereignty and transparency in international technology partnerships.
- **User Rights Protection**: Mandate accountability, strong encryption, and open reporting standards to build user trust.

Trusted Internet Summer School on Internet Governance and International Law is a part of a research project "Satellite Internet: Trust and Data Governance" supported by the Internet Society Foundation