Internet Fragmentation and its environmental impact: A case study of Satellite Broadband[1]

Berna Akcali Gur and Joanna Kulesza

Keywords:

Satellite broadband, Internet Fragmentation, Environmental sustainability, Space Sustainability, Mega Constellations

1. Introduction

The United Nations (UN) has set the goal of achieving meaningful universal digital connectivity by 2030.[2] So that 'anyone, anywhere, regardless of geographic location, socio-economic status, race, gender, or any other differentiating demographic, has access to affordable services and devices to connect to reliable and safe Internet.'[3] Owing to their potential to significantly contribute to this endeavour, the emerging mega satellite constellation ventures are being championed as viable solutions to bridge the digital divide. Led by the US venture Starlink, space-faring nations have embarked on deploying their satellite constellations consisting of thousands of satellites. However, the exponential increase in the number of objects in the Earth's orbits raises concerns about space traffic management, space debris, and the sustainability of orbital resources. Yet, these concerns are fading behind their universal connectivity promise. The existing measures fail to constrain this new competition driven primarily by geopolitical rivalry among major powers and their cybersecurity concerns. The cybersecurity concerns and the resultant national and regional cybersovereignty measures that hinder prioritising orbital sustainability have been identified and scrutinised in Internet governance research as factors contributing to Internet fragmentation.[4] The importance of regulatory and policy measures in addressing the sustainability of the orbital environment is urgent. A well-informed policy and regulatory intervention require a thorough analysis of conflicting interests. In this scenario, the objectives of universal connectivity, cybersecurity measures, and cyber sovereignty, as well as their environmental implications, should be evaluated in relation to their connection to broader Internet governance discussions.

The global Internet governance has been a controversial and disruptive force in international relations.[5] Once envisioned as a global information network, a wide range of concerns associated with maintaining control within state borders and global ideological differences have led countries to adopt restrictive measures.[6] These measures implemented to enhance the ability to control the Internet within national or regional borders, justified under variations of the cyber sovereignty concept, are increasingly transforming the Internet into isolated networks controlled primarily by

[1] This paper is a product of a project funded by the Internet Society Foundation, “Decolonizing the Internet: Global Governance of LEO Satellite Broadband“.

[2] ‘Achieving universal and meaningful digital connectivity: Setting a baseline and targets for 2030’ (ITU and UN Office of the Secretary General’s Envoy on Technology 2022) <https://www.itu.int/itu-d/meetings/statistics/wpcontent/uploads/sites/8/2022/04/UniversalMeaningfulDigitalConnectivityTargets2030_BackgroundPaper.pdf> accessed on 9 October 2022.

[3] ‘The State of Broadband: Accelerating broadband for new realities’ (The Broadband Commission for Sustainable Development, 2022).

[4] L. DeNardis, Interplanetary Internet Governance. (2023, June 22). Retrieved from https://www.cigionline.org/publications/interplanetary-internet-governance, p. 19.

[5] Milton Mueller, Networks and States: The Global Politics of Internet Governance, 2010. MIT Press pg.1

[6] https://www.weforum.org/reports/internet-fragmentation-an-overview

governments or corporations. The recent tensions among the leading powers have intensified the extent of fragmentation. Most significantly, the United States (US) and China regard the use of each other's technology as a national security risk and have placed restrictions on the use of each other's information and communication technologies (ICT).[7] These restrictions and resultant decoupling are extensive and include applications, standards, and physical communication infrastructure.[8] The competition to deploy mega satellite constellations that provide universal broadband services has emerged in this intensified geopolitical setting. China and Russia have already declared that they will now allow services provided by US constellations based on security concerns, and the EU has justified the deployment of its own constellation as part of its endeavour to develop a sovereign, autonomous, and secured connectivity infrastructure.[9]

The perception that ownership and control of communication infrastructure are necessary to ensure sovereignty, autonomy, and security results in fragmentation along national or regional borders. In the case of mega-constellations, it is causing the proliferation of financially dubious ventures that have the potential to have a grave impact on orbital resources. Indeed, space debris and an exponential increase in potential collisions could render the LEO unusable.[10] This will disrupt not only space-based services, including connectivity, but also all potential benefits that could be accessed in space beyond the orbits. It is in the interest of all to ensure sustainable use of the orbital resources for the present and future. It is neither feasible nor desirable for each country to deploy its own mega satellite constellation to ensure digital sovereignty, digital autonomy, or cybersecurity. Given the exponential increase in satellite launches, recognising environmental concerns and regulating the sustainable use of space resources is urgent. One emerging solution is the implementation of national and international debris mitigation measures in line with the United Nations Committee on the Peaceful Uses of Outer Space's (UNCOPUOS) Guidelines for the Long-Term Sustainability of Outer Space Activities published in 2019.[11] In this article, we argue that satellite broadband infrastructure is a complementary part of the global Internet infrastructure rather than a competing alternative and should be governed as such. The equitable and efficient use of space resources and avoiding duplication of efforts and investments is achievable through cooperation between the stakeholders for which existing regional, multilateral and multistakeholder platforms should be utilised.

The second section of this article introduces mega satellite constellations as part of global Internet infrastructure and the current regulatory framework. The third section analyses the causes and implications of global Internet fragmentation and its impact on space-based broadband. In the fourth section, the environmental impact of the Internet is evaluated in the context of mega-constellations. This section emphasises the global efforts to address fragmentation and the potential benefits of these efforts to the environmental risk arising from the proliferation of mega-constellations. This paper reflects results obtained based on a mixed methodology that includes desk research of legal and policy documents, expert interviews with top academics and practitioners in the field, and an international survey of Internet users contacted through ISOC chapters who shared their views on

[7] Berna Akcali Gur, 'Restrictions on Trade in Telecommunications: WTO's cybersecurity conundrum' (2021) 55 Journal of World Trade 3.
[8] Mishra, V. (2023). The Great U.S.-China Tech Decoupling: Perils of Techno-Nationalism | ORF. ORF. Retrieved from https://www.orfonline.org/expert-speak/the-great-u-s-china-tech-decoupling
[9] https://ec.europa.eu/commission/presscorner/detail/en/IP_22_6952
[10] https://www.esa.int/Space_Safety/Space_Debris/ESA_s_Space_Environment_Report_2022
Aaron C. Boley and Michael Byers, 'Satellite mega-constellations create risks in Low Earth Orbit, the atmosphere and on Earth' (2021) 11 Scientific Reports 10642.
[11] COPUOS 62nd session, Report of the Committee on the Peaceful Uses of Outer Space, U.N. Doc A/74/20, 2019.

priorities for the further development and implementation of satellite-based broadband Internet connectivity. The analysis will contribute to the global multistakeholder policy-making efforts and academic literature on Internet governance, focusing on the interplay between the environment and digital communications.

2. Mega Satellite Constellations

2.1 Overview of Mega Satellite Constellations

A basic knowledge of the technology of mega satellite constellations is essential for understanding their regulatory and policy implications.[12] In response to the vast amount of satellite filings, the International Telecommunications Union (ITU) updated its rules in 2019 and defined them as "non-GSO satellite systems having more than one orbital plane where the mutual relative position of each orbital plane and each satellite in its orbital plane is important." In his work, Wood defined them as "a number of similar satellites of a similar type and function designed to be in similar complementary orbits for a shared purpose under shared control."[13] Most mega-constellation satellites are placed in the Low Earth Orbit (LEO) between 300 and 2000 km from the Earth. Their proximity enables them to send and receive signals faster than systems in higher orbits and offer high-speed, low-latency communication services. Low latency is crucial for applications requiring real-time data transmissions, such as voice-over-internet protocol, video conferencing, surveillance and imaging, and remote-controlled machines. Their low altitudes, however, also result in a much smaller coverage area on Earth. That is why a very large number of satellites are required to provide global coverage, whereas three satellites in GEO are sufficient. Compared to larger satellites launched to higher orbits, the smaller satellites used for constellations are typically more affordable because they are quicker to produce and simpler to launch. Their standardised design makes expanding, updating, and renewing the satellite fleet easier. Consequently, operational costs are also decreased.[14]

There are three main components of a satellite broadband system. In addition to the satellite system in orbit, the users will need terminals to connect their Internet-enabled devices to the satellite in closest proximity at a given time. The gateway Earth (ground) station connects the satellite system to the Internet. The satellites' uplink and downlink connections with user terminals and ground stations require a frequency spectrum. The technology requires a ground station within 1000 km of the user terminal to provide seamless connectivity. The dependence on ground stations is anticipated to decrease as inter-satellite links advance technologically. There are multi-orbital systems in which satellites in higher orbits support and enhance constellations in low-earth orbit (LEO satellite constellations). In addition, these systems are connected to cloud infrastructures.[15] Their ground station locations are coordinated with cloud entry points to facilitate faster links and better network management.[16] This is a mutually beneficial arrangement because cloud service providers benefit

[12] Internet Society, Low Earth Orbit Satellites (LEOs) - Internet Society. (2023, February 10). Retrieved from https://www.internetsociety.org/action-plan/leos

[13] Wood, Lloyd, Satellite constellation networks, Internetworking and Computing over Satellite Networks. Springer, Boston, MA, 2003, p.13-34.

[14] Ray, B. (2022). New connectivity options driven by low Earth orbit satellites. ComputerWeekly. Retrieved from https://www.computerweekly.com/feature/New-connectivity-options-driven-by-low-Earth-orbit-satellites

[15] Jordan Novet, 'Google wins cloud deal from Elon Musk's SpaceX for Starlink internet connectivity' (*CNBC.com* 13 May 2021) <https://www.cnbc.com/2021/05/13/google-cloud-wins-spacex-deal-for-starlink-internet-connectivity.html> accessed on 10 July 2022.

[16] Adam Smith, 'Elon Musk's Starlink space internet attached to Microsoft system in breakthrough that could power computers all over the world' (*The Independent* 21 October 2020)

from the connectivity services provided by satellite systems. The use of each component is governed by a different set of laws and regulations that are briefly explained in the next section.

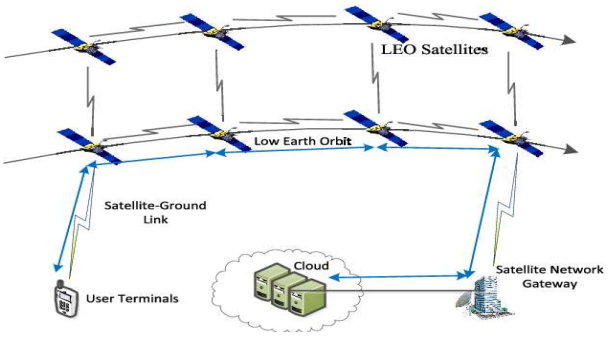
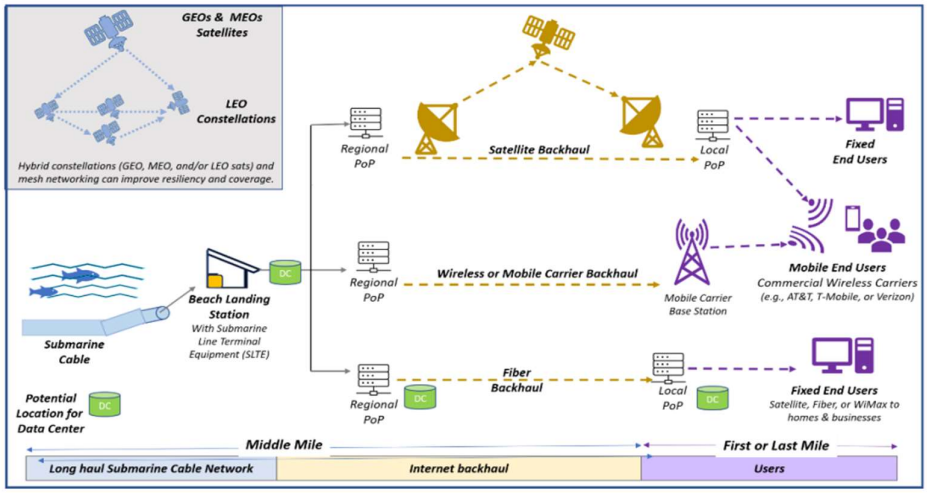


Figure 1. Main Components of a mega constellation system[17]

Satellites have been utilised as communication infrastructures for a long time. The first successful communications satellite deployment was the SCORE project by the Advanced Research Projects Agency (ARPA and later DARPA) in the US in 1958. This government agency is also responsible for the technical foundation of the modern Internet in the 1960s, which was designed to function in emergencies, such as a nuclear attack. [18] Eventually, both the Internet and communication satellites became commercialised.[19] The Internet became an essential utility provided through terrestrial communication infrastructure, while satellites remained important for remote and sparsely populated areas, mobile communications, and emergencies where terrestrial networks are unavailable. However, satellites were not considered a viable alternative to terrestrial infrastructure, especially with the ubiquity of fibre-based networks that enable interference-free, reliable data transmission at light speed.



<https://www.independent.co.uk/space/elon-musk-spacex-starlink-microsoft-azure-b1206439.html> accessed on 20 October 2021

'Technology Futures Spotlight on the technologies shaping communications for the future' (OFCOM, 2021) https://www.ofcom.org.uk/__data/assets/pdf_file/0011/211115/report-emerging-technologies.pdf

[17] Li, Chengcheng, Yasheng Zhang, Renchao Xie, Xuekun Hao and Tao Huang. "Integrating Edge Computing into Low Earth Orbit Satellite Networks: Architecture and Prototype." IEEE Access 9 (2021): 39126-39137.

[18] Mitch Waldrop, 'DARPA and the Internet Revolution' (*Darpa.mil* 2015) available at <https://www.darpa.mil/about-us/timeline/modern-internet> accessed on 10 January 2023.

[19] Walden, Ian in Telecommunications Law and Regulation 5th Ed.Oxford Press

Figure 3.1 Global Internet Infrastructure and the role of communication satellites[20]

The progress in wireless mobile technologies has further enhanced Internet-enabled social, industrial, and governmental functions. Until the emergence of mega-constellations, the role of satellites in global Internet infrastructure was considered limited. The exact scope of their role and viable business models are still being determined as the industry matures. Early entrants to the market are pursuing different strategies, with some focusing on providing backhaul services for wireless communications and network redundancy, while others are focusing on connectivity for IoT devices through a multi-orbit system. [21] The trajectory suggests that the LEO satellite technology will become a complementary part of the global communications network consisting of cable and wireless infrastructures rather than replace existing systems.

2.2. Cybersecurity of Mega Satellite Constellations

Cybersecurity is the "security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that cyberspace"[22] It is one of the most divisive topics in international platforms, causing a stalemate, which led to the proliferation of protective measures at national and regional levels. The national and regional data protection regimes and agreements on cybersecurity-related standards impact how communications networks are set up and protected. As global reliance on satellite broadband increases and broadband use for a broader range of functions becomes necessary, assessing the existing cybersecurity arrangements for critical infrastructure is also becoming urgent.[23]

Integrating mega satellite constellations into the existing Internet infrastructure exposes it to the current global cyber threat landscape and the problem of indeterminacy of international norms in that area. Also, increased reliance on LEO satellite constellations for broadband services is expected to expand the cyber threat landscape due to cyber vulnerabilities specific to their technologies and how they function.[24] For example, some of their new technologies, such as software-defined satellites and lasers for data transfers, increase the risks.[25] Another security concern is the interconnectivity between mega satellite constellations and 5th Generation (5G) mobile networks. 5G is designed to

[20] Lori W Gordon and Karen L Jones, 'Global Communications Infrastructure: Undersea and Beyond' (The Aerospace Corporation Centre for Space Policy and Strategy 2022) <https://csps.aerospace.org/papers/global-communications-infrastructure-undersea-and-beyond> accessed on 30 January 2023.

[21] Daniel Voelsen, 'Internet from Space' (Stiftung Wissenschaft und Politik Research Paper 6, April 2021) < https://www.swp-berlin.org/en/publication/satellite-internet> accessed on 24 February 2022.
'Perspectives on LEO Satellites' (Internet Society November 2022) < https://www.internetsociety.org/resources/doc/2022/perspectives-on-leo-satellites/> accessed on 1 December 2023.

[22] 'Definition of Cybersecurity – Gaps and overlaps in standardisation' (ENISA December 2015) <https://www.enisa.europa.eu/publications/definition-of-cybersecurity > accessed on 23 February 2023.

[23] Roy Balleste, 'The Law of Space Cyber Operations: Gripping Mysteries, Entangled Frontiers, and Security Challenges' (2022) 13 Journal of Law, Technology, & the Internet 146.

[24] David Livingstone and Patricia Lewis, *'Space, the Final Frontier for Cybersecurity?'* (2016) Chatham House Research Paper, International Security Department.
Pingyue Yue et al., "On the security of LEO satellite communication systems: Vulnerabilities countermeasures and future trends" (*ArXiv>EESS* 2022) < https://arxiv.org/abs/2201.03063 > accessed on 20 February 2023.

[25] 'EUSPA: the gatekeeper to a secure EU Space Programme' (*European Union Agency for the Space Programme (EUSPA) News* 21 April 2022) < https://www.euspa.europa.eu/newsroom/news/euspa-gatekeeper-secure-eu-space-programme > accessed on 30 April 2022.

enable advanced mobile applications and services, industrial transformation, massive machine-to-machine communications, and time-critical applications by providing higher speed, capacity, low latency, and high reliability. The number of connected people, devices, governments, and critical infrastructures will increase exponentially with 5G-enabled applications, with cloud services playing a pivotal role. The international nature of satellite communications and their connection to these wireless terrestrial infrastructures and services expand the threat landscape. More thorough analyses will emerge as the use of these systems becomes ubiquitous. However, the ongoing geopolitical obstacles to tackling global cybersecurity will likely prevent fully realising this technology's benefits and effective utilisation.

In the absence of a multilateral regulatory framework, countries and regions are responding to the risks on their terms, in line with their cyber policies, most of which have become more and more protectionist over the years. The EU Agency for the Space Program has confirmed that data transmitted via space technologies is vulnerable to cyberattacks. In 2023, its Network and Information Systems Directive (NIS2) was amended to include the space sector and imposed stricter cybersecurity requirements on the organisations affected. There is a proposal to further regulate the security-related aspects of space-based services through the Critical Entities Resilience Directive.[26] The increased use of satellites for broadband communications has also been recognised in the UK's Space Industry Regulations of 2021, which has a dedicated cybersecurity section.[27]

The US Space Policy Directive-5 of 2017 outlines best practices for the cybersecurity of space systems, recognising that these systems are vulnerable to the same cybersecurity risks as terrestrial systems. The directive implements a comprehensive, standards-based approach that emphasises supply chain security, encryption, and physical security of components. There is also discussion about whether space systems should be regulated as the 17th critical sector by the Cybersecurity and Infrastructure Security Agency (CISA).[28] In April 2022, Congress introduced the Satellite Cybersecurity Act, which recognises the reliance on national and foreign commercial satellites as a matter of national security.[29] China and Russia have stated they would not allow Starlink to provide services within their borders. At the same time, Chinese authorities claimed it is a potential "serious challenge to all countries in defending their cyberspace sovereignty and protecting their information security."[30] Recent reports of SpaceX CEO Elon Musk singlehandedly deciding to prevent a Ukrainian drone attack by disabling Starlink satellites over the targeted area add to these concerns.[31] These early responses of the major space-faring nations to this technology indicate that they all recognise the cybersecurity risk associated with it and infer a link between cyber vulnerability and the risks it poses to national infrastructure with foreign ownership.

2.3. The Regulatory Framework of Mega Satellite Constellations

The mega-satellite constellations are subject to distinct sets of normative frameworks. The fundamental principles of Outer Space apply to the use and exploitation of space resources, including

[26] European Commission, 'Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities' COM(2020) 829 final

[27] United Kingdom, The Space Industry Regulations 2021 No 792, Chapter 3.

[28] Edward Swallow and Samuel Visner, 'It's time to declare space systems as critical infrastructure' Politico 2 April 2021

[29] S.3511 – US Satellite Cybersecurity Act 117th Congress (2021-2022)

[30] Li Xiaoli, 'Starlink's expansion, military ambitions alert world' China Military Online 5 May 2022 http://eng.chinamil.com.cn/OPINIONS_209196/Opinions_209197/10152439.html

[31] Reuters. (2023). Musk says he refused Kyiv request for Starlink use in attack on Russia. Reuters. Retrieved from https://www.reuters.com/world/europe/musk-says-he-refused-kyiv-request-use-starlink-attack-russia-2023-09-08

the deployment, control and operation of all spacecraft. The international and national telecommunications laws and regulations apply to the coordination of high-frequency radio waves and orbital positioning to enable seamless communication of all satellites in orbit with the Earth. These are most relevant to the sustainable use of orbital resources and state responsibility. The third is domestic laws and regulations that regulate companies providing broadband services and importing and selling telecommunications equipment. The international law principles that are being interpreted and negotiated with respect to cyberspace are also relevant. These norms are most pertinent to cybersecurity and cyber sovereignty concerns associated with the mega satellite constellations. A detailed analysis of the applicable legal framework is beyond the scope of this paper. However, a general understanding is necessary to explain that mega satellite constellation ventures rely on existing normative frameworks that regulate all phases of their operation, which falls short of mitigating their environmental impact.

2.3.1. Mega Satellite Constellations as Outer Space Infrastructures

The Outer Space Treaty (OST), signed in 1967 under the United Nations, is the first treaty that established rules for the exploration and use of space. It is now considered a part of customary international law, so its fundamental principles are binding upon all countries, including those that have not signed this treaty.[32] Four other treaties and numerous UN resolutions based on the OST principles make up the main body of space law. The drafters of the OST did not foresee the commercialisation of outer space or space debris becoming a problem. However, some of its fundamental principles require equitable use of space resources, especially Article IX, that requires activities to be conducted sustainably, without causing harm and with due regard to the interests of others. Considered together with the principle that space is the province of all humankind, the freedom of exploration and use of outer space by all states without discrimination, and the principle of non-appropriation of outer space, this can be interpreted to require the utilisation of space resources to be limited by considerations of space sustainability. [33]

Four other treaties, other UN conventions and General Assembly resolutions have developed the OST principles. These instruments, some of them non-binding, address a more comprehensive range of issues such as preserving space and Earth's environment, liability for damages caused by space objects, dispute resolution, information sharing about potential dangers in outer space, using space-related technologies, and international cooperation. The countries ensure that the launch and operation of commercial communication satellites must adhere to these internationally agreed norms and principles. One fundamental principle is that states have jurisdiction over their space objects and are responsible for licensing and registering them. National registries conduct the registration. This information is made public through the public registry maintained by the UN. The UN registries provide global transparency, which acts as a confidence-building measure among nations, and it is also necessary to manage space traffic and prevent space collisions. Even with a handful of projects underway, the brief life span of satellites in mega-constellations and their frequent de-orbits are expected to cause a significant increase in space debris, which is already a problem.[34]

States are also directly responsible for all their national space activities. It is their responsibility to ensure that all their activities are conducted for peaceful purposes and in accordance with international law. So, they have a strong incentive to supervise and regulate private space

[32] Francis Lyall and Paul B. Larsen, *Space Law: A Treatise*, 2nd Ed., p.73

[33] Berna Akcali Gur and Joanna Kulesza, What We Owe Each Other: Equitable Access to Secure, Affordable, and Reliable LEO Broadband Satellite Services - A Development Perspective' GigaNet Annual Symposium 2022.

[34] Bernhard, P., Deschamps, M., & Zaccour, G. (2023). Large satellite constellations and space debris: Exploratory analysis of strategic management of the space commons. Eur. J. Oper. Res., 304(3), 1140–1157. doi: 10.1016/j.ejor.2022.04.030

enterprises. The state's responsibilities expand to international liability. The launching state, which may differ from the registering state, is liable for damage to other states, their citizens, and their property. So, mega satellite constellation ventures are subject to a wide range of domestic laws and regulations in all phases of their operations. Most licensing and authorisations are obtained in the pre-launch phase. Rules and regulations about the in-orbit phase are primarily an extension of state oversight and control responsibility as also prescribed in international law. The particulars vary depending on which jurisdiction these companies are operating from. The recently intensified concerns about the exponential increase in space objects have led space-faring countries to adopt legal measures in orbit tracking for purposes of traffic management to avoid collisions. The end-of-life de-orbiting procedures are also regulated at the domestic level, and these are considered one of the key measures to mitigate the space debris problem.

Despite the apparent risks, these instruments do not contain binding norms that can limit states from launching mega satellite constellations into space. However, they form the basis of what space-faring nations do to mitigate the adverse effects of their space activities. According to space agencies and space technology experts, these measures are insufficient to stop the emerging threat to the orbital environment.[35]

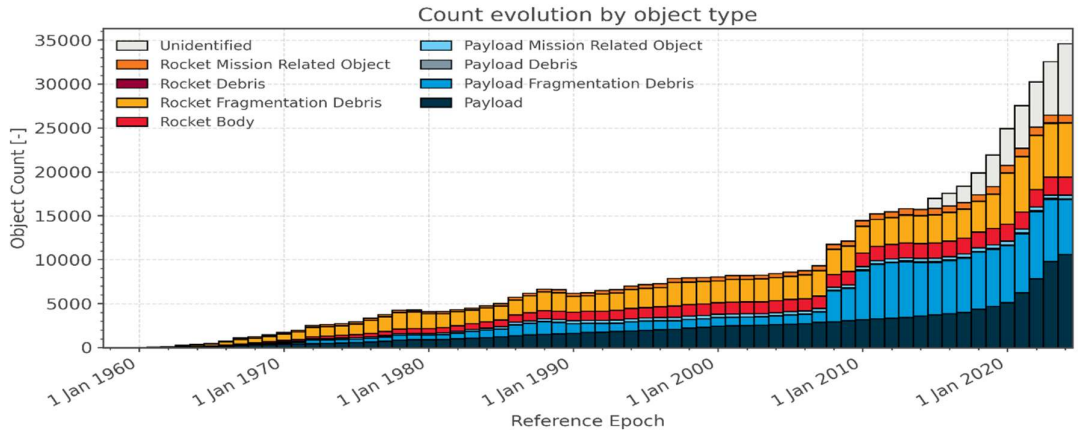


Figure: The exponential increase in the number of space objects[36]

Due to the exponential increase in the number of space objects, space traffic has become more challenging to manage, and more collisions are anticipated. The space environment is becoming more prone to collisional cascading, which means that once a certain threshold is reached, the total volume of space debris will continue to grow. This is because collisions create additional debris, leading to more collisions creating a cascading effect.[37] Such a catastrophe may render not only LEO but almost all space resources inaccessible for all - even for future generations.

2.3.2. Use of Radio Frequency by Mega Satellite Constellations

The frequency spectrum and satellite orbits are limited natural resources that must be used rationally, efficiently, and economically. The ITU coordinates and manages the orbital positions and the radio frequencies satellites require to communicate with the Earth. The rules and regulations

[35] Venkatesan, A., Lowenthal, J., Prem, P., & Vidaurri, M. (2020). The impact of satellite constellations on space as an ancestral global commons. Nat. Astron., 4, 1043–1048. doi: 10.1038/s41550-020-01238-3

[36] ESA Space Debris Office, 'ESA'S Annual Space Environment Report' GEN-DB-LOG-00288-OPS-SD, 12 September 2023

[37] Donald J. Kessler, 'Collisional cascading: The limits of population growth in low earth orbit' (1991) 11 Advances in Space Research 12 (63-66) https://doi.org/10.1016/0273-1177(91)90543-S.

governing these, as well as the rights and obligations of ITU Member States, are outlined in the CS, ITU Convention (CV), the Radio Regulations (RR), and the Rules of Procedures (RoP), all of which have treaty status. The Radio Regulations (RR) provides the fundamental framework for global coordination and management of the radio-frequency spectrum. Through representation by a national administrative body, Satellite operators submit their requests to the Master International Frequency Register (MIFR). The MIFR is a record of frequency assignments and orbital positions that are in use or planned for future use. Member states are responsible for ensuring that their rules and regulations align with these principles. The filing requests of countries are coordinated with previously determined frequency allocations, which were established through earlier planning and coordination processes. These processes involved regular negotiations between national administrations and the ITU. The ITU's role is to facilitate fair access to these resources. The registration system at the ITU is significant because of the shortcomings of the UN registration system for mega satellite constellations. According to a 2022 COPUOS background paper, there are inconsistencies in state practice among the 72 signatories to the Registration Convention, and there is no specific mechanism for large constellations.[38] Therefore, some satellites remain unregistered, and the registries do not require information on which satellites are deployed as part of a constellation.

Until recently, ITU regulations pertaining to small satellites in Low Earth Orbit (LEO) were less stringent and did not necessitate international coordination. However, with the emergence of mega-constellations, the ITU revised its regulations at the World Radio Conference in 2019 to address pressing concerns. For the first time, the term 'satellite constellation' was defined, and most constellation projects were included in the redefined requirement for the coordination procedure. A novel phased approach was adopted, stipulating that project deployment must be completed within seven years, with 10% within two years and 50% within five years. This approach aims to align the Master International Frequency Register with the actual deployment of non-Geostationary Orbit (non-GSO) satellite systems. It also seeks to strike a balance between preventing spectrum warehousing, ensuring the proper functioning of coordination, notification and registration mechanisms, and meeting operational requirements related to the deployment of non-GSO systems.

The ITU's proficiency in managing spectrum and associated orbital resources and member states' familiarity with its system were crucial in implementing these vital steps towards a more equitable allocation system for LEO and associated frequencies. While not flawless, this represents a significant advancement and underscores global governance mechanisms' importance and continued relevance despite prevailing scepticism towards multilateral platforms. However, incorporating orbital environmental concerns into the ITU-R system will require broader agreement among members.

2.3.2. Mega Satellite Constellations as Internet Service Providers

Internet Service Providers operating mega satellite constellations could be expected to comply with the domestic measures regulating digital data flows, data collection, storage, and processing, some of which also call for data localisation. It is widely accepted that these regulations must be followed by all multinational corporations that have access to or handle data.

The delivery of satellite services within a specific country is governed by that nation's legal and regulatory framework, a concept known as landing rights. The individual countries determine the terms of these landing rights. For instance, ground stations must be established at least every 1000 km and require authorisation from each relevant jurisdiction. Additionally, a license to utilise the frequency spectrum must be obtained. If services are provided directly to consumers, an Internet service provider license is likely also necessary. The scope of these licenses and authorisations varies

[38] background paper regarding the registration of large constellations in accordance with the Convention on Registration of Objects Launched into Outer Space and the non-binding General Assembly Resolution 1721 B (XVI) in 2022

with the business model. For example, Starlink's direct-to-consumer model would likely necessitate all licenses, whereas OneWeb, which primarily serves incumbent telecom operators and governments, would be subject to a different, narrower set of requirements. Furthermore, the importation of user terminals is subject to the import requirements of national authorities. As current trends suggest, there may be some harmonisation of these rules at the regional level or among like-minded states. However, we are still in the early stages, and it remains to be seen what the future holds.

These domestic regulations are expected to adhere to the international law commitments of each country. The market access commitments under the World Trade Organisation agreements and preferential trade agreements will be of utmost relevance. While the range of commitments will differ from country to country, regulatory measures are generally expected to be transparent, reasonable, objective, and impartial in sectors where specific commitments have been made. Consequently, licensing, procedural requirements, technical standards, and procedures should not be employed to establish unnecessary trade barriers. Trade agreements have increasingly been utilised to promote environmental objectives between trading partners in recent years.[39] These environmental provisions may also become relevant in licensing procedures of services provided by mega satellite constellations.

3. Internet Governance and Mega Satellite Constellations

The policy and regulatory framework that apply to satellite broadband systems sit at the crossroads of international and domestic law and other regulatory instruments that concern Internet governance. It is a complex normative matrix. Ensuring that it serves the interest of specific communities and their members has been difficult because navigating it requires capacity and resources to allow stakeholders to interact in a variety of venues actively. The environment has been a peripheral policy concern in the regulatory efforts.

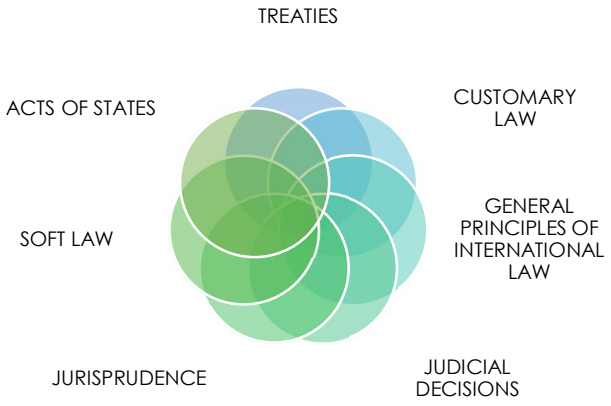


Fig. 6. Sources of international law applicable to satellite-facilitated broadband Internet.[40]

The mega satellite constellations will provide Internet services, a communication medium that has been designed decentralised to prevent threats to the network and its resources. So, there is no single point of control that, if hacked, could destroy the whole global network. This mirrors the original network design aim of constructing a worldwide communication infrastructure that could

[39] Environment and Regional Trade Agreements - OECD. (2023, March 30). Retrieved from https://www.oecd.org/env/environment-and-regional-trade-agreements.htm
[40] For reference see e.g. James Crawford, Brownlie's Principles of Public International Law (9th edn) OUP 2019.

withstand a single, most likely nuclear, attack.[41] This decentralised design is based on decentralised infrastructure (local software and network backbone architecture) and a democratic, peer-to-peer, trust-based mechanism. All network nodes have equal status, and their successful operation is founded on the predicament that actors will diligently perform their duties when it comes to the everyday operation of the network. Trust has always been the global digital economy's lifeblood. This egalitarian, distributed design varies from other known governance models, which are built on authority, power, and enforcement, whether public or private. Despite the absence of either of these components, the Internet continues to operate, and its governance model has proven vital to its success.

ITU member countries first acknowledged the network's social, economic, and political potential in 2003. The World Summit on the Information Society (WSIS), convened by the ITU, was the first formal intergovernmental summit to examine the potential issues that the global network brings to international and local governments.[42] It founded the Working Group on Internet Governance (WGIG), a select group of telecommunications and international relations experts assigned by member states, to define the preliminary questions and opportunities presented by this global communication phenomenon to international policies. The WGIG issued a report in 2005 that described "Internet governance" as "the development and application by governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programs that shape the evolution and use of the Internet," a definition later adopted by the WSIS in its 2005 Tunis Agenda for the Information Society.[43]

This definition represents the vast range of standard-setting and decision-making bodies and procedures crucial to the global network's day-to-day operation. It also expresses the multistakeholder model, which is essential to Internet governance. While "multistakeholder" is extensively used in international relations theory and practice, official UN papers typically refer to an "Internet governance multistakeholder approach." The Tunis Agenda also underlines the need for the multistakeholder approach as a tool for "better coordination of the operations of international and intergovernmental organisations, as well as information sharing among themselves."[44] Also, Europe views the multistakeholder model as key to the Internet's continued success.[45] In a recent study, the multistakeholder model was suggested as the most suitable model to tackle the space debris problem

[41] For a review of Internet's history and origins see: Balleste, R. (2015). 'Internet Governance. Origins, Current Issues and Future Possibilities'. Rowman and Littlefield, 11-15.

[42] Most notable documents developed in the original WSIS process include: WGIG, (2005). Report of the Working Group on Internet Governance. Available at: www.wgig.org/docs/WGIGREPORT.pdf. Retrieved Feb. 8th, 2023. WSIS (2003). Declaration of Principles; Building the Information Society: a global challenge in the new Millennium. Available at: http://www.itu.int/wsis/docs/geneva/official/dop.html. Retrieved Feb. 8th, 2023.
WSIS (2003). Plan of Action. Available at: http://www.itu.int/wsis/docs/geneva/official/poa.html. Retrieved Feb. 8th, 2023. WSIS (2005). Tunis Agenda For The Information Society. Available at:
http://www.itu.int/wsis/docs2/tunis/off/6rev1.html. Retrieved Feb. 8th, 2023.

[43] ITU, WSIS Tunis Agenda, Para. 34 reads: "A working definition of Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet'.

[44] ITU, WSIS Tunis Agenda, para. 37.

[45] See e.g. European Commission, Communication From The Commission To The European Parliament, The Council, The European Economic And Social Committee And The Committee Of The Regions, Internet Policy and Governance Europe's role in shaping the future of Internet Governance (Text with EEA relevance) /* COM/2014/072 final */, EUR-Lex - 52014DC0072 - EN. (2023, July 09). OPOCE. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52014DC0072 with a clear statement: "The European Commission is firmly committed to the multistakeholder model of Internet governance."

and sustainable management of LEO, which would allow deliberation among communities of technical, economic, legal and political backgrounds.[46]

3.1. Internet Fragmentation and Mega Satellite Constellations

Splitting the global network into smaller, national, or regional intranets governed by national authorities or regional intergovernmental organisations has been an alternate response to the global Internet governance paradigm. This issue is frequently raised in the ongoing “Internet fragmentation” or "splinternet" discussion.[47] Internet fragmentation refers to the Internet becoming divided into multiple non-interoperable and disconnected "splinternets". It can be a 'total or partial lack of connectivity, happen either at the transport or the application layer, be caused by technical, commercial or political factors, and affect the Internet either as a technical infrastructure, a digital public sphere, or both.' The challenge of Internet fragmentation is intrinsically entangled with geopolitics. Countries aim to create their own "splinternets" to exert greater control over the inward and outward flow of data. This also gives them more control over their citizens' access to information and allows them to manage Internet use in line with their national security interests. Some governments and regional organisations have pursued this policy goal while remaining interoperable with the global web. Some examples are the Great Chinese Firewall, the more recent Russian RuNet project, and the latest EU draft policy on DNS4EU.[48]

Other entities, such as companies or governmental organisations, also create their own "splinternets" to protect sensitive information, improve network security, or other reasons. On the flip side, splinternets can lead to the use of technologies that are not interoperable, cybersecurity standards and regulations, which may undermine collaboration on and consistency of global security efforts, which are already under pressure from geopolitical tensions. Indeed, decoupling at the infrastructure level, such as the 5G crisis and the competition between China and the US over submarine cable routes, are manifestations of Internet fragmentation and part of a broader geopolitical struggle where both countries seek to expand their economic and strategic interests.[49]

Countries are expanding their security measures to include restrictions on the flow of ICTs goods and services and investment, especially from rival countries. In this context, a country's ability to control and mitigate the risks arising from technological dependence is also regarded as a crucial element of ensuring cybersecurity and cybersovereignty. Technological dependence refers to a country's reliance on technology developed and controlled by other countries. The global crisis surrounding the 5G

[46] Daniel Lambach and Luca Wesel, ‘Tackling the Space Debris Problem: A Global Commons Perspective’ (2021) Conference Paper, 8th European Conference on Space Debris, ESA Space Debris Office

[47] Mueller, M. (2017). Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace (Digital Futures). Polity.

[48] Sherman, J. (2022). Reassessing RuNet: Russian internet isolation and implications for Russian cyber behavior. Atlantic Council. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior. Retrieved Feb. 8th, 2023.Whalebone (2023). ‘Press Release: DNS4EU. The European Commission plans to onboard 100 million people to a new EU-based DNS internet infrastructure.’ Available at: https://www.whalebone.io/post/press-release-dns4eu . Retrieved Feb. 8th, 2023.
Wagner, J., (2017). ‘China’s Cybersecurity Law: What You Need to Know’. The Diplomat. Available at: https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know. Retrieved Feb. 8th, 2023. See also: Press, L. “A New Chinese Broadband Satellite Con-stellation”, CircleID. Available at: http://www.circleid.com/posts/20201002-a-new-chinese-broadband-satellite-constellation/.

[49] C. Kavanagh, Wading Murky Waters: Subsea Communications Cables and Responsible State Behaviour | UNIDIR. (2023, September 21). Retrieved from https://www.unidir.org/publication/wading-murky-waters-subsea-communications-cables-and-responsible-state-behaviour

rollout has been an example of this global dynamic, as numerous states restricted or banned the use of Chinese hardware and software in their wireless communications infrastructure. Dependence on foreign technology companies for national Internet infrastructure is linked with cybersecurity risks and control over how national data is collected, stored, transferred, and used. Cybersecurity, technological and cyber sovereignty concerns have all played a role in determining these measures. Internet fragmentation emerges as both the goal and the result of such policies and resultant norms.

The primary purpose of the mega satellite constellations is to provide broadband access. The recurring association of sovereignty with ownership and control of them, in some cases to the exclusion of those controlled by companies of other states, is one of the latest examples of sovereignty and security concerns associated with global infrastructure for Internet access and the resultant fragmentation. A similar example is submarine cables. Submarine cables are critical infrastructures that carry vast amounts of data and information across the world's oceans and seas. They are owned and operated by various entities, including private companies, governments, and consortia. The political and strategic implications of their ownership, operation, and maintenance of submarine cables are significant, especially since it has been revealed that some countries sought to control or influence the flow of information across submarine cables to advance their national security interests or to exert greater control over their citizens' access to information.[50] So, countries with the financial means have been seeking to establish their own submarine cable networks and submarine cable landing stations strategically. The objectives are various, ranging from gaining competitive advantage in the global economy, enhancing military capabilities, reducing dependence on other countries for access to information and mitigating their potential use for espionage and cyberattacks by others. They are considered strategic assets, the control of which is essential. There are strong parallels between the geopolitics of the submarine cables and the emerging mega satellite constellations from a cybersovereignty perspective, whereas the same dynamics are causing strategic competition in space, which may result in irreversible environmental damage.

3.2. Cybersovereignty and Mega Satellite Constellations

Public and private companies from leading countries compete to extend their influence and presence in cyberspace, resulting in ownership and control structures that widen the gap with others who rely on their goods and services. These deepening dependencies and the consolidation of power in data-based international economic activities are becoming more challenging to counterbalance. They are regarded as challenges to protect national interests and security. In the past decade, domestic policies and measures aimed at mitigating these dependencies or their perceived adverse effects have been associated with the principle of state sovereignty that, in the words of the EU authorities, includes the "right to control the social, economic, and security impact of ICTs and other reliant technologies as an extension of their political and territorial sovereignty."[51] This particular objective is referred to as cybersovereignty, although the national interpretations of this concept and the measures they implemented to achieve it vary considerably around the globe.

These variations and jurisdictional uncertainties surrounding other layers of the Internet had less impact on telecommunications, which functions as the physical layer of cyberspace. Telecommunications services have always remained tightly regulated as there is universal recognition

[50] Snowden revelations.

[51] Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means. Research Policy, 52(6), 104765. doi: 10.1016/j.respol.2023.104765, see also: European Parliament, Foreign interference in all democratic processes in the European Union - Wednesday, 9 March 2022. (2023, September 21). Retrieved from https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_EN.html

of sovereign control over the telecommunications infrastructure, most located on national territories.[52] Using satellite broadband presents a challenge for cybersovereignty policies in telecommunications because it requires minimal or no terrestrial infrastructure. Nevertheless, the domestic measures, which apply to territorial infrastructure and domestic Internet service providers, will be expected to apply to its use. While the international regulatory framework requires authorisation and licensing procedures to provide satellite services in a particular country, implementing cybersecurity measures is a separate issue. As with most ICT advancements, defining and implementing policies in a timely manner is a challenge. The lack of a comprehensive global legal framework, primarily due to the growing economic and ideological rivalry between the US and China, increased the need for domestic solutions.

One prevalent response of significant economies to cyber sovereignty concerns associated with the emerging mega satellite constellation ventures has been to invest in their own mega satellite constellation. They justified the considerable investment in these elaborate projects with reference to the importance of sovereign control over these infrastructures. The planned EU mega satellite constellation IRIS2 stands for "Infrastructure for Resilience, Interconnectivity and Security", a space-based secure communication system for the benefit of EU citizens.[53] The UK has also invested in a mega-constellation, OneWeb, which has been described as a sovereign global satellite system and a significant strategic investment.[54] It has since received investment from India's Bharti Group and merged with EUTELSAT, an incumbent satellite operator. Among shareholders, there are Japanese, South Korean, and American companies. It has also been reported that OneWeb will use the cloud services of Amazon Web Services (AWS), a US company.[55] Despite the multinational shareholding structure, the UK retains a special share in the company, which allows it to exercise some exclusive rights, including its use for national security purposes and a range of other national security-related rights, i.e., over the security standards of the network. Also, the UK ensured that it remains the preferred location for future satellite launches and procurement for manufacturing.[56] According to this example for the UK, control, rather than sole ownership, is sufficient to ensure the security of a (sovereign) satellite system. As expected, China, the country that has erected the "Great Firewall" to control access to information and protect national security interests, has filed applications for more than one mega satellite constellation project at the ITU. Reportedly, Russia also has plans to deploy its mega satellite constellation, which will further the goals it aims to achieve with the Sovereign Internet Law, which allows it to partition itself from the rest of the Internet. Telesat is credited with enhancing Canadian sovereignty and national security.[57] The sovereign mega satellite constellation discourse validates the perception that Internet connectivity using non-national technology or infrastructure is untrustworthy and a security risk, a significant drive behind Internet fragmentation.

[52] Nanette S. Levinson and Derrick L. Cogburn, 'The Next Turn in Internet Infrastructure Governance' in Laura DeNardis and others (eds), *The Turn to Infrastructure in Internet Governance* (Palgrave Macmillan 2016)
[53] https://defence-industry-space.ec.europa.eu/eu-space-policy/iris2_en
[54] House of Commons Science and Technology Committee, 'UK space strategy and UK satellite infrastructure: Government Response to the Committee's Second Report' HC 1258 Published on 30 March 2023 Published by authority of the House of Commons
[55] https://telecoms.com/520618/oneweb-bags-aws-deal-as-cloud-security-comes-under-scrutiny/
[56] Department for Business, Energy & Industrial Strategy, 'OneWeb merger with Eutelsat' News story 26 July 2022 https://www.gov.uk/government/news/oneweb-merger-with-eutelsat
[57] https://www.telesat.com/press/press-releases/telesat-applauds-the-government-of-canada-on-the-release-of-its-new-defence-policy/

4. Environmental impact of Mega Satellite Constellations

Global Environmental Governance refers to the collective systems, organisations, policies, norms, procedures, and standards that oversee the processes of global environmental protection.[58] It involves interactions at multiple levels among various stakeholders, including governmental bodies, the private sector, and civil society. These stakeholders engage with each other in both formal and informal settings to develop and implement policies in response to environmental needs and societal inputs. Implementation at global and local levels is key to its success. Recently, it has been considered in relation to its role in achieving sustainable development, exemplified in the work of the United Nations Environment Programme and the United Nations Development Programme. Indeed, environmental sustainability is connected with the social and economic aspects of sustainable development. depend on effective decision-making processes, robust institutions, policies, laws, standards, and norms.

International Environmental Law is comprised of bilateral and multilateral international agreements that set out the rights and obligations of states concerning environmental protection and sustainable use of natural resources dedicated to the preservation and enhancement of the environment. The norms are primarily aimed at mitigating the adverse effects of human activity on climate and the environment. It plays a vital role in setting the legal basis for the norms, procedures and standards that are the product of global governance mechanisms. Although there are varying approaches, it is generally accepted that the orbital environment should not be considered outside the scope of environmental law or other initiatives that support and regulate the sustainable use of resources.[59]

4.1. Space Sustainability and Maga Satellite Constellations

The space-based communications infrastructure has a renewed significance with the emergence of the mega satellite constellations, which are able to provide broadband Internet services because of their proximity to Earth. However, their elaborate infrastructure, more precisely the number of satellites required for these ventures, is causing legitimate environmental concerns, shadowing their universal connectivity potential. The Earth's orbital space environment constitutes a finite resource that is being exploited by an industry present only in a handful of space-faring countries and is evolving at a fast pace. The ongoing competitiveness risks the long-term sustainability of outer space activities is defined as "the ability to maintain the conduct of space activities indefinitely into the future in a manner that realises the objectives of equitable access to the benefits of the exploration and use of outer space for peaceful purposes, to meet the needs of the present generations while preserving the outer space environment for future generations."[60] Yet the international regulatory framework falls short of ensuring this objective. The policymakers and regulators are faced with the arduous task of balancing the competing interests at national, regional and international levels.

[58] Adil Najam, Mihaela Papa and Nadaa Taiyab, *Global Environmental Governance: A Reform Agenda* (2006) International Institute for Sustainable Development (IISD), pg 3.

[59] April G. Apking, 'The Rush to Develop Space: The Role of Spacefaring Nations in Forging Environmental Standards for the Use of Celestial Bodies for Governmental and Private Interests' (2005) 16 Colorado Journal of International Environmental Law & Policy 429

Francis Lyall and Paul B. Larsen, Space Law: A Treatise, 2nd Ed., p.245

[60] The Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space and the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Outer Space Treaty)

Even with a handful of projects underway, the brief life span of LEO satellites and their frequent de-orbits is expected to cause a significant increase in space debris, which is already a problem. The proliferation of mega satellite constellations and the increased risks of collision and interference with the operation of space objects may affect the long-term sustainability of space activities. The environmental dangers of such space debris are myriad, including light pollution that would hinder future scientific discovery. Just as worrying are satellite re-entries from the mega-constellations, which could deposit hazardous levels of alumina into the upper atmosphere. The resulting solar radiation would have pernicious consequences for the environment.[61] A 2017 study showed that adding a mega-constellation to the space environment results in a 50 per cent increase in the number of catastrophic collisions – involving the complete destruction of a satellite – over 200 years, with potentially severe consequences for other satellites and the services they provide to the ground, as well as financial implications for the operators and that the current measures are not sufficient to prevent this.[62] So, space traffic is becoming more challenging to manage, and more collisions are anticipated. And the space environment is becoming more prone to collisional cascading. Such a catastrophe may render not only LEO but almost all space resources inaccessible for all - even future generations.

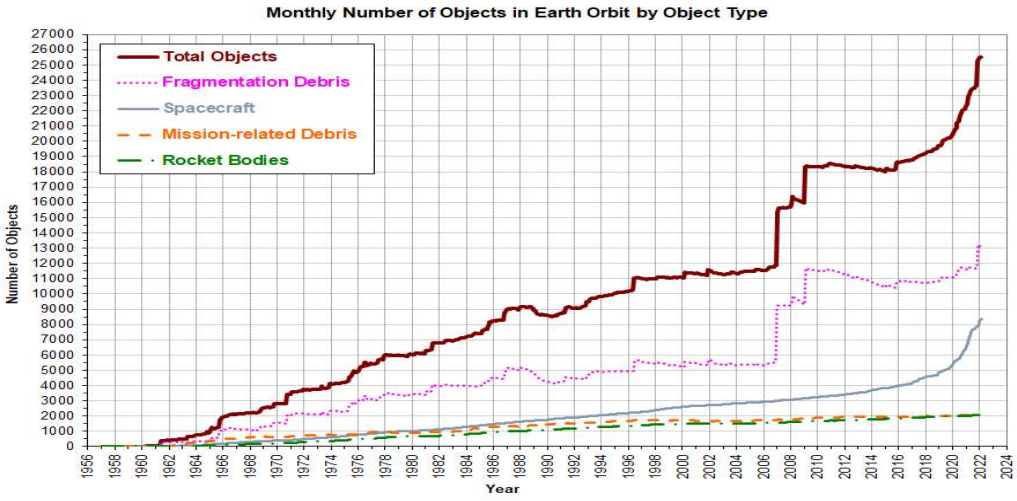


Figure 3. Chart showing the number of objects >10 cm in LEO.[63]

A survey conducted by the authors of this article among Internet Society Chapters revealed an awareness of environmental concerns. The answer to a question on the most important global concern regarding the implementation of LEO-based technologies was very clear. Environmental concerns around space debris have been indicated as needing prompt policy response. Among other selected policy items to be addressed, the respondents noted in equal proportions space collision,

[61] Rajeev Suri, 'What's the environmental impact of space debris and how can we solve it?' World Economic Forum https://www.weforum.org/agenda/2022/07/environmental-impact-space-debris-how-to-solve-it/Jul 13, 2022

[62] Ramon J. Ryan, 'The Fault in Our Stars: Challenging the FCC's Treatment of Commercial Satellites as Categorically Excluded from Review under the National Environmental Policy Act' (2020) 22 Vanderbilt Journal of Entertainment and Technology Law 923

University of Southhampton, 'Biggest ever space debris study highlights risk posed by satellite 'mega-constellations' 19 April 2017 News https://www.southampton.ac.uk/news/2017/04/space-debris-mega-constellations.page

[63] NASA Orbital Debris Program Office

spectrum interference, colonisation of space resources, and securitisation of Low Earth orbit, with no concerns expressed about the potential negative impact on astronomical observations.

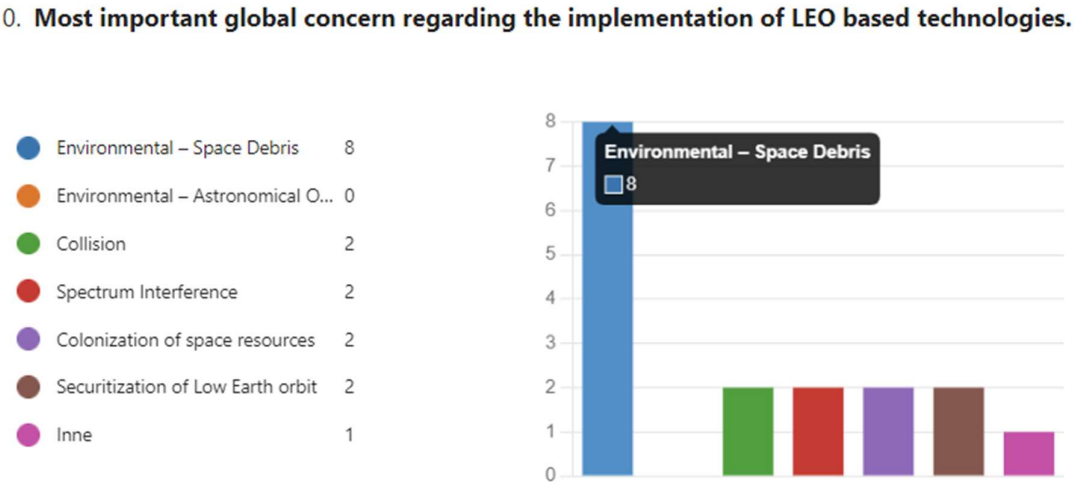


Figure 4. Most important global concern.[64]

In 1987, the UN Brundtland Commission defined sustainability as to the ability of humans to meet their needs without compromising the ability of future generations to meet theirs. One of the main goals of sustainability is to protect and conserve the environment from the negative impacts of human activities so that natural resources are maintained or restored for the long term. Recently, The Committee on the Peaceful Uses of Outer Space has examined the long-term sustainability of outer space activities from various angles. The Working Group on the Long-term Sustainability of Outer Space Activities of the Scientific and Technical Subcommittee has built on these previous efforts and other relevant initiatives to develop voluntary guidelines. These guidelines aim to provide a comprehensive approach to promoting the long-term sustainability of outer space activities and enhancing the safety of space operations.[65] Space activities are essential tools for realising the achievement of the Sustainable Development Goals. Hence, the long-term sustainability of outer space activities is of interest and importance for current and emerging participants in space activities and future generations. Strategic competition in an industry, the economic viability of which is uncertain, does not excuse undertaking such a risk.[66] The justification of these projects is the need to own and control Internet infrastructure to ensure cyber sovereignty and cybersecurity. This issue will be best addressed at multistakeholder platforms, though their success has been questionable so far.

4.2. Greening the Internet & Fragmentation

The mainstream provision of broadband internet connectivity is a novel prospect. The interplay between universal connectivity, sustainable development, and greening the Internet has preoccupied the agenda of governments, international organisations, primarily the International Telecommunications Union (ITU) and the UN, and multistakeholder platforms such as the Internet Governance Forum (IGF) and private companies. The urgency of solutions is evident. The carbon

[64] Berna Akcali Gur, Joanna Kulesza, 'ISOC Chapters Survey', https://www.cyber.uni.lodz.pl/fileadmin/LODZ_CYBER_HUB/OUTPUT_1_ISOC_chapter_survey_and_review.pdf
[65] UN, 'Guidelines for the Long-term Sustainability of Outer Space Activities'
[66] Miles Lifson and Richard Linares, 'Is there enough room in space for tens of billions of satellites, as Elon Musk suggests? We don't think so' Op-Ed SpaceNews 4 January 2022 https://spacenews.com/op-ed-is-there-enough-room-in-space-for-tens-of-billions-of-satellites-as-elon-musk-suggests-we-dont-think-so/

footprint of ICTs is estimated to account for about 3.7% of global greenhouse emissions and is predicted to double by 2025 and produce 14% of global greenhouse gas emissions by 2040.[67] Therefore, the role that ICTs can play in promoting environmental sustainability and facilitating sustainable development should be considered with respect to their negative impact on the environment. The ITU recognised the significance and set the ICT industry target to reduce emissions by 45% by 2030.[68] The promise of facilitating global universal connectivity justifies the deployment of mega satellite constellations. It should also be considered with respect to their impact on the environment, whereas a set of balancing policies is necessary.

Internet fragmentation can have an environmental impact because creating "splinternets" often leads to inefficiencies, including in the architecture of the underlying infrastructure. The increased need for data centres to comply with domestic data localisation measures can increase energy consumption and carbon emissions.[69] Generally, the need for additional infrastructure and resources to support the "splinternets" often increases energy consumption and carbon emissions.[70] The importance of minimising the environmental impact of digitalisation and internet c connectivity has been recognised. The efforts to help 'green the internet' refer to the process of making the Internet more environmentally sustainable. This can involve using renewable energy sources to power data centres, improving energy efficiency in data centres, promoting sustainable practices in the production and disposal of electronic devices, and promoting sustainable practices in the production and disposal of electronic devices used to access the Internet.[71] From an Internet governance perspective, promoting interoperability and collaboration between different parts of the Internet, as well as developing consistent standards and regulations for cybersecurity across different regions and countries, is often deemed the preferable solution.[72] These efforts are closely linked with the cyber security and sovereignty justifications countries put forward for investing in their own mega satellite constellations, and their involvement would enhance the discussion on using these infrastructures efficiently.

5. Conclusion

Advancements in most information and communication technologies (ICTs) are commonly evaluated in the context of their potential implications for global power dynamics. Notably, the emergence of mega satellite constellations is viewed as a strategic investment, serving dual purposes: bolstering a

[67] Sarah Griffiths, 'Why your internet habits are not as clean as you think' (bbc.com 6 March 202) <https://www.bbc.com/future/article/20200305-why-your-internet-habits-are-not-as-clean-as-you-think>
'The Carbon Footprint of the Internet (Climate Impact Partners 22 April 2021) <https://www.climateimpact.com/news-insights/insights/infographic-carbon-footprint-internet/>

[68] 'ICT industry to reduce greenhouse gas emissions by 45 percent by 2030' (Press Release ITU, 27 February 2020) < https://www.itu.int/en/mediacentre/Pages/PR04-2020-ICT-industry-to-reduce-greenhouse-gas-emissions-by-45-percent-by-2030>

[69] Dlzar Al Kez, Aoife M. Foley, David Laverty, Dylan Furszyfer Del Rio, Benjamin Sovacool, 'Exploring the sustainability challenges facing digitalization and internet data centers'(2022) 371 Journal of Cleaner Production 133633, https://doi.org/10.1016/j.jclepro.2022.133633.

[70] William J. Drake, Vinton G. Cerf and Wolfgang Kleinwächter, 'Internet Fragmentation: An Overview' January 2016 World Economic Forum Future of the Internet Initiative White Paperhttps://www.weforum.org/reports/internet-fragmentation-an-overview

[71] Policy Network on Environment and Digitalisation, 'Recommendations on Using Digitalisation for Our Common Future' (2022) Wäspi, F. (Ed.) Internet Governance Forum.

[72] Joseph Bocchiaro, 'Sustainable ICT: Mitigating the Carbon Footprint of the Digital Economy Through Standards' (2022) 1 Journal of Research and Innovation 8.

nation's presence in space and enhancing its influence and control over the critical infrastructure that underpins the global internet.

The escalating geopolitical competition among nations has led to a phenomenon of internet fragmentation, wherein countries are driven to expand their space-based internet infrastructure. Regrettably, this endeavour comes at a cost, as the proliferation of satellite constellations amplifies the environmental footprint associated with internet connectivity.

It is imperative that the impetus to assert dominance in Earth's orbits, already heavily congested, is tempered with an awareness of the need to preserve a sustainable orbital environment for the benefit of future generations. In this regard, the environmental initiatives spearheaded by global multistakeholder internet governance platforms can offer valuable insights and guidance for shaping environmentally responsible and sustainable governance frameworks for outer space, particularly as they pertain to space-based internet infrastructure.

The overarching objective of policies and ensuing actions should centre on fostering innovative space solutions that bridge the global digital divide while also nurturing sustainable development. Striking a harmonious balance between promoting the utilisation of space resources and safeguarding them for the welfare of future generations is essential. This complex balancing act necessitates careful consideration of the heightened global tensions surrounding cybersecurity and the resulting fragmentation of the internet landscape.

In addition to the imperative of balancing sustainability and innovation in space-based internet infrastructure, it is equally crucial to address the critical aspects of international liability regimes, insurance mechanisms, and proactive prevention strategies. These elements are essential components of a comprehensive framework for responsible governance in the realm of cyberspace and outer space. As a result, three following points are due further research:

1. International Liability Regimes: The rapid expansion of space-based internet infrastructure introduces new complexities regarding liability for any potential mishaps or conflicts in outer space. It is imperative that the international community engages in dialogue to establish clear and equitable liability regimes that outline responsibilities and consequences for actions or accidents in space. Such regimes should be informed by the principles of fairness, accountability, and adherence to international law. This would provide a legal framework to address disputes and allocate liability in a transparent and just manner.

2. Insurance Mechanisms: As the stakes in space-based activities rise, the need for robust insurance mechanisms becomes evident. Governments, private companies, and international organizations involved in space endeavors should consider the development of insurance schemes tailored to the unique challenges of the space domain. These mechanisms should not only cover potential damages but also incentivize safe practices and responsible conduct. Moreover, they can serve as a financial safeguard against unforeseen events, thereby encouraging investment in sustainable space initiatives.

3. Proactive Prevention: Prevention is often more cost-effective and less disruptive than responding to incidents or disputes after they occur. Therefore, proactive measures for preventing conflicts, accidents, and environmental harm in space should be a central focus. This includes the promotion of international cooperation, transparency, and responsible behavior in space activities. Establishing norms and guidelines for responsible conduct, risk assessment, and exchange of good practices can contribute significantly to reducing the potential risks associated with space-based internet infrastructures as a peril to sustainable development and environmental protection.

In conclusion, the pursuit of a sustainable and responsible approach to space-based internet infrastructure governance should encompass not only environmental concerns and technological innovation but also the crucial elements of international liability regimes, multistakeholder internet governance, and proactive prevention strategies. These considerations collectively form a

comprehensive framework that ensures the long-term viability, security, and equitable use of outer space resources for the benefit of present and future generations.