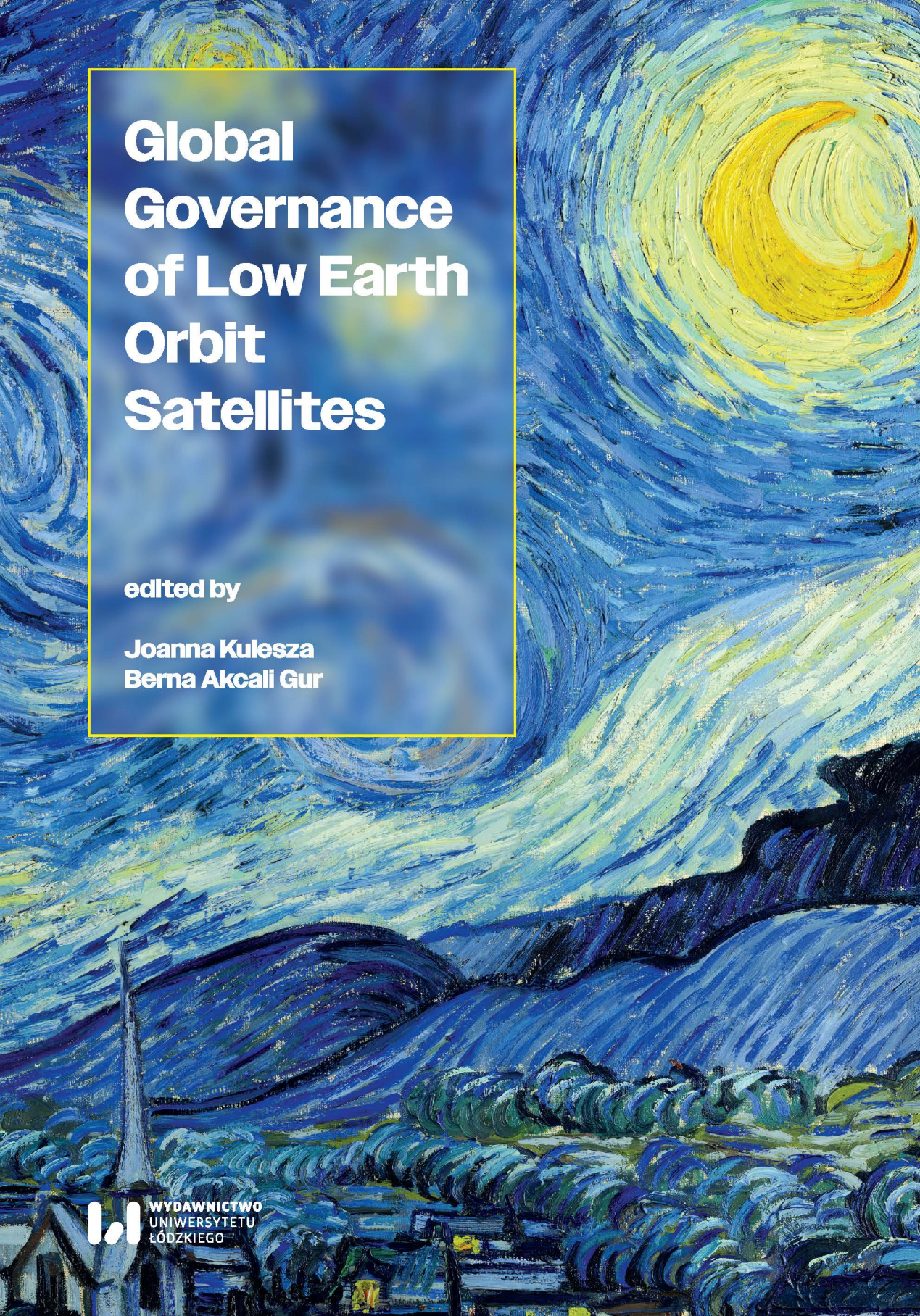
Global Governance of Low Earth Orbit Satellites

edited by

Joanna Kulesza
Berna Akcali Gur



WYDAWNICTWO
UNIWERSYTETU
ŁÓDZKIEGO

Global Governance of Low Earth Orbit Satellites

WYDAWNICTWO
UNIWERSYTETU
ŁÓDZKIEGO

Global Governance of Low Earth Orbit Satellites

edited by

Joanna Kulesza
Berna Akcali Gur

WYDAWNICTWO
UNIWERSYTETU
ŁÓDZKIEGO

Łódź 2025

Joanna Kulesza (ORCID: 0000-0003-0390-6062) – University of Lodz
Faculty of Law and Administration
Department of Public International Law and International Relations
90-232 Lodz, 8/12 Kopcińskiego St.

Berna Akcali Gur (ORCID: 0000-0003-4861-5533) – Queen Mary University of London
Centre for Commercial Law Studies, 67-69 Lincoln's Inn Fields, London WC2A 3JB
United Nations University – Institute on Comparative Regional Integration Studies
Potterierei 72, 8000, Brugge

REVIEWERS
Roxana Radu, *Jamal Shahin*

INITIATING EDITOR
Monika Borowczyk

PUBLISHING EDITOR
Aleksandra Urzędowska

TYPESETTING
PAJ-Press

TECHNICAL EDITOR
Wojciech Grzegorczyk

COVER DESIGN
Polkadot Studio Graficzne Aleksandra Woźniak, *Hanna Niemierowicz*

Cover Image: Vincent van Gogh, *The Starry Night*, 1889, WikiCommons

© Copyright by Authors, Lodz 2025
© Copyright for this edition by University of Lodz, Lodz 2025

This document is an output from a project funded by the Internet Society Foundation. It was supported by the Internet Society Foundation project G-202307-12461 "Satellite Internet: Trust and Data Governance" and builds upon research completed under project G-202107-04813 "Decolonizing the Internet: Global Governance of LEO Satellite Broadband"

The Open Access version of this book has been made available under a Creative Commons Attribution-NonCommercial-No Derivatives 4.0 license (CC BY-NC-ND)

https://doi.org/10.18778/8331-719-9

Published by Lodz University Press
First edition. W.11711.25.0.K
Publisher's sheets 13.0; printing sheets 13.625

ISBN 978-83-8331-718-2
e-ISBN 978-83-8331-719-9

Lodz University Press
90-237 Lodz, 34A Jana Matejki St.
www.wydawnictwo.uni.lodz.pl
e-mail: ksiegarnia@uni.lodz.pl
phone 42 635 55 77

Table of Contents

https://doi.org/10.18778/8331-719-9.01

Preface

Joanna Kulesza, Berna Akcali Gur

This book is the culmination of our, the co-editors of this volume, project on the Global Governance of Low Earth Orbit Satellite Broadband, generously funded by the Internet Society Foundation as part of its transformative Decolonizing the Internet program. Since 2023, the project has embarked on a pivotal second phase, focusing on the crucial themes of "Trust and Data Governance".

In the first phase, we explored the implications of developed states' current geopolitical and economic dominance in setting standards for LEO satellite broadband in developing countries. We examined the critical policy issues that governmental and civil society actors must urgently address in response to the rapid development of satellite-based internet access, which resulted in the publication of an open-access report and dedicated policy recommendations for civil society and governmental actors. During this phase, we had the unique opportunity to work in parallel with a dedicated Internet Society expert group, which focused on researching the technical implications and potential of LEO satellite systems. The cross-pollination of our collaborative efforts proved invaluable, enriching the depth and breadth of our research. The project's second phase reviewed how international and multistakeholder forums can effectively tackle transnational data governance concerns, promote open and trustworthy internet policy objectives, and bridge the capacity divide between the Global North and the Global South in the context of newly enhanced satellite internet capabilities. Over the past four years, we have actively participated in various forums, including the Internet Governance Forum (IGF), the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), and RIPE Network Coordination Centre (RIPE NCC) meetings, as well as the annual European Society of International Law (ESIL) and RightsCon to discuss and share our research. Throughout this journey, we have had the privilege of collaborating with and learning from numerous experts, chiefly Dan York, who led the Internet Society team researching LEOs, and Larry Press, Jonathan Liebenau, Celestine Rabouam, Roxana Radu, Dmitry Epstein, Jane Coffin, Peter Micek, Jamal Shahin

and others. We also collaborated with several institutions, primarily the University of Lodz Faculty of Law and Administration, the Global Internet Governance Academic Network (GigaNet), and the United Nations University Institute on Comparative Regional Integration Studies (UNU-CRIS). We are grateful for their support and collegiality.

In this second phase of the project, one of the highlights was the opportunity to host a group of interdisciplinary experts and young researchers from around the globe for a week-long face-to-face meeting in Lodz, Poland. During this meeting, we engaged in discussions on the way forward for sustainable internet infrastructure development. Each day began with a keynote address by an expert. Impressed by the quality of the papers presented at the workshop, we decided to compile selected papers into this edited volume. We invited other experts we had met along the way to contribute. The result is this volume, which we hope will serve as a valuable resource for policymakers, researchers, and anyone interested in the governance of LEO satellite broadband and its implications for global internet governance.

https://doi.org/10.18778/8331-719-9.02

Contributors

Dr. Roy Balleste is a tenured Professor of Law at Stetson University College of Law, where he also serves as the Director of the Dolly & Homer Hand Law Library. He specialises in cyberlaw and space law, focusing on astronautical ethics, cybersecurity law, internet governance, space cybersecurity, and space law. Professor Balleste holds multiple advanced degrees, including a PhD in Space Cybersecurity from Capitol Technology University, a J.S.D. in Intercultural Human Rights from St. Thomas University, and an LL.M. in Air and Space Law from McGill University. He has been recognised for his contributions to the field, including receiving the Nicolas Mateesco Matte Space Law Prize at McGill University.

Jason Bonsall is an academic affiliated with both the University of Nevada, Reno, and the University of Padova. His research has primarily focused on the intersection of technology and society, with particular emphasis on exploring pathways to enhance global internet connectivity. Notably, he published an article comparing machine learning algorithms to address political polarization in the United States and authored his thesis on the societal benefits of community network connectivity.

Dr. Laetitia Cesari is a researcher and a legal practitioner working on the law and policy of outer space, with a focus on security and safety aspects, and particularly cybersecurity of space systems. Among other missions, she works for a law firm in Paris and carries out research for various international organisations. Laetitia earned a doctorate of law from the University of Luxembourg. Prior to her current position, Laetitia worked in the space industry, specifically in telecommunications. Before that, she supported the work of national authorities on space-related topics.

Dr. Berna Akcali Gur is a legal scholar specialising in public international law. Her research focuses on public international law, world trade law, and EU Law implications of the advancements in information communication technologies. She is currently an Associate Research Fellow at the United Nations University Institute on Comparative Regional Integration Studies (UNU-CRIS) and the module convenor for Outer Space Law at the Centre for Commercial Law Studies, Queen Mary University of London. Before her academic career, she practised

law in Istanbul, New York, and London. She holds an LL.B. from Ankara University, an LL.M. from the University of Pennsylvania, and a Ph.D. from King's College London.

Mallory Knodel is the Executive Director of the Social Web Foundation. She focuses on human rights and a people-centred approach to technology implementation, with particular emphasis on open protocols, encryption, and censorship circumvention. Mallory is also the co-chair of the Human Rights Protocol Considerations research group of the Internet Research Task Force and an advisor to the Freedom Online Coalition. She has a physics and mathematics background, and is a PhD candidate at the NYC Courant School of Mathematics.

Dr. Joanna Kulesza is an Assistant Professor of International Law at the University of Lodz, where she also serves as the Executive Director of the Lodz Cyber Hub. Her research focuses on the application of international law in cyberspace, cybersecurity, and internet governance. She has published extensively on these topics and is involved in various international research projects.

Dr. Jonathan Liebenau is Reader in Technology Management at the London School of Economics and Political Science (LSE). He specialises in the fundamental concepts of information and the challenges and opportunities of information and communication technology (ICT) in economic development. Dr. Liebenau has authored or edited several books and numerous publications. He has provided consultancy services to leading companies, strategic government agencies, and international organisations. His work often focuses on the intersection of technology management, innovation, and economic development. He also leads LSE Tech, a research group at LSE's Department of Management that is active in the areas of internet and communications economics, policy, and strategy.

Célestine R. Rabouam is a PhD student at the French Institute of Geopolitics (IFG) and a researcher at the GEODE (Geopolitics of the Datasphere) research centre. Her research focuses on the geopolitical and technical challenges posed by the growing hybridisation of terrestrial and satellite telecommunications systems in the Canadian Arctic, particularly in Nunavut. She examines the impact of satellite constellations, such as Starlink, on technological dependencies and the digital organisation of networks in the Arctic. Her work highlights how these developments are affecting the political and economic landscape of the region.

Monika Stachoń is an expert specializing in strategic analysis of security and cybersecurity. She is currently responsible for shaping the long-term vision of the Polish Space Agency. Her research interests include cybersecurity regulations, national strategies in cyberspace, and the use of space technologies in the context of security and defense. She is the author of numerous expert studies and academic articles on critical infrastructure, crisis management, cybersecurity policies, and digital diplomacy. She is preparing a doctoral dissertation on Iran as a state sponsor of cyberterrorism.

Dan York is a leading expert in the field of Internet technology and communications. He is currently the Senior Director of Internet Technology

& Communication of Internet Society where he works on Internet resiliency and has led the organization's analysis of Low Earth Orbit (LEO) satellite systems, seeking to understand the benefits and challenges of this new way to provide Internet access and connect the unconnected. He has a strong background in technology and has been involved in various aspects of internet infrastructure, including DNS security, IPv6 deployment, and the development of open standards. He is also an active writer and speaker, contributing to numerous publications and conferences on Internet technology and policy topics.

https://doi.org/10.18778/8331-719-9.03

Introduction

Berna Akcali Gur, Joanna Kulesza

Space-based Internet connectivity has garnered significant attention in recent years, primarily after the successful deployment of Starlink, the first mega constellation project to achieve global coverage. This milestone has catalyzed a competitive international landscape, with major space-faring nations committing substantial resources to develop independent satellite networks. Simultaneously, private enterprises, particularly within the United States, are engaging in rival projects, further intensifying the race to establish next-generation global broadband infrastructures. From its beta testing phase, Starlink's services have been crucial in diverse scenarios, including disaster and conflict zones, as well as remote and sparsely populated areas where terrestrial infrastructure would be impractical or too costly. As impressive use cases increased, so did the intensity and depth of debates among a wide range of stakeholders regarding the potential implications of this technology, particularly for global power dynamics, security and cybersecurity, sustainable use of space resources, and sustainable development. Civil society, businesses, policymakers, and regulators have all had to rapidly develop policies and take necessary steps to safeguard their interests. Simultaneously, researchers and policy experts from diverse backgrounds have engaged in analysis from the perspective of their expertise, including political economy, communications theory, legal and policy analysis. This book contributes to these discussions by bringing together policy experts, civil society, leading scholars and emerging scholars from diverse backgrounds. This book aspires to reach a broad audience by providing a comprehensive insight into the impact of space-based broadband Internet connectivity. We believe each chapter will captivate and engage readers eager to broaden their knowledge and delve deeper into the subject matter.

Space-based Internet connectivity has advanced significantly with the successful deployment of satellite constellation systems in low Earth orbit (LEO). These systems have the potential to profoundly transform global Internet access by bridging the digital divide and reaching communities in rural or isolated regions. The United Nations (UN) Sustainable Development Goals recognise that

improved Internet access can boost local economies by enabling e-commerce, remote work, and access to global markets while supporting essential services such as education and healthcare, which increasingly rely on digital connectivity. Additionally, space-based Internet can enhance resilience in regions affected by natural disasters or conflict zones, ensuring continuous communication and access to information when other options fail. This technology ensures that even the most remote parts of the world can be connected, which is crucial for achieving universal Internet access. However, the rapid expansion of space-based Internet services has created an urgent need for a review of existing policies and regulations to manage spectrum allocation, orbital slots, and space debris. International cooperation is essential to address these challenges and ensure equitable access. The contributing authors to this volume agree that while it is each jurisdiction's prerogative to determine policies that serve their specific interests, there is a critical need for deliberation on various aspects of this technology at the international level.

Starlink, a Space Exploration Technologies Corp. (SpaceX) subsidiary, has leveraged its parent company's advanced rocket systems and mass satellite manufacturing capabilities to achieve remarkable success. Unlike previous attempts that faltered mainly due to financial constraints, Starlink has deployed thousands of satellites in low Earth orbit (LEO) with unprecedented speed and efficiency, thanks to SpaceX's enabling technologies. Additionally, Starlink achieved diplomatic success by negotiating the placement of ground stations across various jurisdictions, a technical requirement for global coverage. This rapid progress caught competitors, including private companies in the US and other space-faring nations, off guard. As more companies and countries venture into space-based Internet projects, they have become a central feature of the New Space Race. The increasing number of space actors and private companies defines this new era. The Moon and Mars exploration remain distant prospects for many; space-based connectivity concerns everyone, whether space-faring or not. The future of global connectivity may well depend on how effectively these challenges are addressed. Each chapter analyses a different aspect of these challenges.

Compelled by the success of Starlink, several other mega constellation projects are being developed to provide global Internet coverage. As of the time of publication, its closest competitor, Eutelsat OneWeb, had deployed 648 satellites in low Earth orbit (LEO). Eutelsat OneWeb's major shareholders include Eutelsat, a publicly traded company listed on the Euronext Paris stock exchange, the UK Government, and Bharti Global, an Indian company. Another US-based company, Amazon's Project Kuiper, is in the process of deploying a competing system. Canada-based Telesat's Lightspeed project is working on a constellation system in LEO after securing financing from the Government of Canada and the Government of Quebec. China is also entering the market with several satellite constellation projects, including Guowang, Hongyan and Hongyun. These are part of China's strategic efforts to enhance its space-based Internet capabilities and compete globally in the satellite communication sector. The European Union has also approved an

EU-based mega constellation, Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS2). It aims to provide secure communication services to the EU and its Member States and broadband connectivity for European citizens, private companies, and governmental authorities. It will support various applications, including border surveillance, crisis management, and secure communications for EU embassies. This new wave of satellite constellations is poised to revolutionise global connectivity. At the same time, they highlight the perceived need to own and control infrastructure for security and cybersecurity concerns by those with the financial and technological capacity to do so. Meanwhile, others are left to figure out how to protect their interests in the global power dynamics where they are merely the users. The chapters in the book reflect both sides of this dynamic.

The book adopts a global governance perspective, focusing on the analysis and understanding of the rules and processes that govern space-based Internet connectivity as a global issue transcending national borders. A balanced approach is pursued, recognizing both the transformative benefits and inherent associated risks. Concerns regarding the space environment, cybersecurity, regulatory control, geopolitical tensions, and equitable distribution are discussed. Although there is not a dedicated chapter, the threat caused by the rapid increase in satellite deployments to the sustainability of Earth's orbits has been raised by the editors and Dan York. Indeed, as thousands of satellites are launched at an accelerated pace, the risk of collisions and the proliferation of space debris grow, further complicating orbital safety—especially in the absence of a globally governed traffic management system. Nevertheless, its significance in enabling connectivity even in the most remote regions remains undeniable, serving as a crucial foundation for universal Internet access—an essential public resource for accessing both public and private goods and services in today's increasingly interconnected world—making it a continued focal point.

The chapters encompass contributions from multiple disciplines, including political science, international relations, economics, and international law, to elucidate the complex interactions between various actors. In addressing the pertinent challenges, the roles, effectiveness, and influence of different actors—such as states, intergovernmental organisations, private companies, and civil society—are examined, exploring how global governance mechanisms can effectively address these issues. Collectively, the essays aim to inform policymaking at national, regional, and global levels by providing insights into how global cooperation can be enhanced and how international institutions can be more effective in addressing shared problems to promote global stability and prosperity. Despite its ambitious goals, the book is a concise contribution and does not claim to address all problems comprehensively. One significant issue, the editors wish to include in a future volume is the light pollution exacerbated by mega-constellations, which disrupts astronomical observations and limits scientists' ability to study the universe. Consequently, several topics are not included in this volume, it is not exhaustive.

The sections are organised into three parts. The first part comprises two sections. The first section introduces the modernised satellite broadband technology and contemporary policy issues, primarily from a global connectivity perspective. The second section analyses historical events and trends, providing insights into how past economic policies and developments influence present-day issues. The second part is dedicated to the security implications of space-based Internet. The three essays are connected by considering cybersecurity as a key security concern. This link also establishes how the digitalisation of communication technologies played a central role in the perception of space-based connectivity. The third part comprises selected essays on regional approaches to space-based Internet. These essays were presented at the Trusted Internet Summer School on Internet Governance and International Law (SSIGIL) in 2024, hosted by the University of Lodz at the Faculty of Law and Administration premises as part of a research project supported by the Internet Society Foundation. Postgraduate students from three continents presented and discussed their work on satellite broadband technology throughout the week. These essays are followed by a commentary by an established policy professional advocating for the Internet Governance multistakeholder model as the model to follow to address global policy issues.

The first contribution by Dan York, a world-renowned Internet technology expert who led a LEOs project team at the Internet Society Foundation. The team researched the use of mega satellite constellation systems in LEO for Internet access and developed a "Perspectives on LEO Satellites" document outlining opportunities, challenges, and enduring questions. The team comprised experts from around the world, representing various stakeholder interests. Their work was guided by the goal of user benefit and addressing the global digital divide. Building upon this project and his extensive expertise in communication technologies and non, D. York introduces contemporary satellite broadband technology and potential policy issues and responses. D. York's contribution delivers a comprehensive outline of the technology and its implications, paving the way for essays focusing on more specific aspects. Following this invaluable contribution is another by Jonathan Liebenau, who explores the satellite industry from three perspectives: economics, history, and business practices. The essay traces the historical context of satellite development from the International Geophysical Year (1957–1958) onwards. In examining the economic relationships within the satellite industry, he highlights the complexities compared to traditional capitalist markets. Lastly, he focuses on the business models of satellite companies and their government predecessors, comparing various revenue-generating approaches. The paper also discusses the broader relationship between digital infrastructure and satellite Internet, providing insights into the economic trade-offs. Although often perceived as a technological marvel, constellation technology has existed for a considerable time. Its financial viability has only recently been realised due to advancements in enabling technologies. J. Liebenau is well placed to conduct this analysis as his expertise on the subject is over 30 years, starting with his research into the LEO

industry in the late 1990s in a project aimed to inform the UK Civil Aviation Authority and their National Air Traffic Control Service, which wanted an assessment as to whether and when space-based infrastructures in LEO would be reliable as well as financially feasible to integrate into their existing communications systems.

Section 2 comprises three essays by leading scholars that focus on the security-related aspects of satellite constellation technology. These essays complement each other by addressing the broader implications of mega-constellations for security on Earth and in the Earth's orbits, as well as the security of human space exploration. These essays illustrate how overlapping and diverging security and cybersecurity concerns impact our present and future activities on Earth, in orbit, and in outer space beyond the Earth's orbits. The section begins with Roy Balleste's insights on the cybersecurity implications for human space exploration in LEO and beyond. He contends cyber operations present significant risks to current and future peaceful space endeavours. The dynamic cybersecurity landscape necessitates new practices and the establishment of a cybersecurity framework guided by the wisdom of scholars who long ago recognised the benefits of space exploration and the evolving nature of peace and security. According to the author, immediate solutions lie in a new cybersecurity framework anchored in Outer Space Law, which will inspire the development of innovative legal principles. R. Balleste's previous research focused on several areas, including astronautical ethics, which explores the ethical dimensions of space exploration; cybersecurity law, particularly in the context of space operations; internet governance, which investigates how internet policies and regulations impact global cyberspace; and space cybersecurity, which addresses the unique cybersecurity challenges posed by space activities and the development of legal norms to protect these operations this work is informed by his extensive knowledge in cyberlaw, space law, and cybersecurity.

Following this, Laetitia Cesari underscores the importance of space security in LEO, given the critical role of space-based assets in supporting essential services, economic activities, and national security. In this chapter, she explores how LEO satellite constellations revolutionise operations for space operators and users, highlighting the increased collision risks posed by the growing population of operational satellites and space debris. The chapter discusses the significance of dual-use space systems in diplomatic dialogues. It offers reflections on potential governance pathways, including law and diplomacy, while acknowledging the complexity of finding straightforward solutions. L. Cesari recognises that addressing these challenges requires coordinated efforts from various stakeholders. States must foster international cooperation and ensure compliance with international obligations. Diplomacy and the rule of law are essential to enhancing space security and protecting activities in LEO. This work is informed by L. Cesari's prior research, which includes numerous publications aimed at improving the understanding and governance of space activities and ensuring their long-term sustainability and security.

The contribution by the editors, J. Kulesza and B. Akcali Gur concentrates on possible domestic governance strategies for satellite broadband, aiming to tackle cybersecurity concerns while leveraging these services to aid developmental objectives. This essay expands upon their prior research regarding space-based connectivity, highlighting the importance of information communication infrastructure and broadband Internet access in achieving the UN sustainable development goals, as mentioned in the Preface. They incorporate a discussion on multistakeholder processes for global cybersecurity efforts and the impact of substantial gaps in expertise, technical capacity and the lack of transparency in effective participation in these processes. The authors argue that the prevailing cybersecurity policies will shape LEOs' future role in global Internet access, international cybersecurity and equitable global digital development.

In Section 3, the book introduces essays on regional approaches to LEOs. These essays were selected from those presented at SSIGIL by postgraduate students representing a diverse range of countries across three continents. The first essay is by Célestine R. Rabouam. She conducted her work in the Canadian Nunavut region—the gradual dependence on Starlink and its impact on Canada's digital organisation of arctic territories. During her PhD research, she made sure to grasp local dynamics during her extended stays in this region. The editors have been impressed with her work, consulted her as an expert for their project, and are very happy that her contribution has found its place among the others. Her research focuses on the geopolitical and technical challenges posed by the increasing hybridisation of terrestrial and satellite telecommunications systems in the Canadian Arctic, particularly in Nunavut. She examines the impact of satellite constellations, like Starlink, on technological dependencies and the digital organisation of networks in the Arctic. Her work highlights how these developments affect the region's political and economic landscape.

This essay is followed by Monica Stachoń's essay on the use of LEO satellites for cybersecurity and broader security strategies of authoritarian regimes, using Iran as a case study. It delves into the impact of space-based systems in LEO on national security, technological advancements, environmental monitoring, and political stability. This study underscores how space technologies, particularly LEO satellites, can become essential to authoritarian states' security frameworks, enhance internal surveillance and intelligence activities, and foster independent cyber capabilities. M. Stachoń's expertise in cybersecurity and her educational background in Iran studies make her well-suited for this analysis. The article provides insight into the space capabilities and use cases of non-aligned space-faring nations that do not have the capacity to deploy a mega constellation system, offering a more holistic picture of the LEO environment. This section is particularly significant given that Iran experienced the unauthorised provision of satellite broadband services by Starlink to protestors whose internet access was obstructed by the government during the 2022–2023 civil unrest. The incident led to a legal reiteration of jurisdictional requirements for licensing and authorisation of foreign service providers

but also sparked a parallel discussion on the human rights implications of these established rules.

The third essay, written by Jason Bonsall, examines why some countries, despite standing to gain significantly from satellite broadband services due to its rapid deployment potential and ability to bridge the digital divide caused by limited infrastructure, are hesitant to authorise and license these services. His article is informed by his previous research on decolonial theory and highlights national regulatory frameworks and geopolitical factors as significant obstacles to the broad adoption of this technology. His analysis focuses on the impact of LEO satellite broadband on connectivity initiatives and the telecommunications industry across the continent by considering the 2Africa connectivity initiative by Meta and the United Nations' Universal and Meaningful Digital Connectivity by 2030 target. He concludes this contribution with a case study that contrasts Nigeria, where Starlink is authorised, and South Africa, where it is not, illustrating different approaches to achieving global connectivity and emphasising Starlink's unique role in the telecommunications sector.

In Section Four, we have a commentary by Mallory Knodel. Drawing from her years of expertise in Internet governance and multistakeholderism platforms, M. Knodel draws parallels between multistakeholder governance models for the Internet and their applicability for space-based infrastructures. The author argues that it is the best-suited model for satellite broadband governance. Her intervention is informed by her work as co-chair of the Human Rights Protocol Considerations research group of the Internet Research Task Force and advisor at the Freedom Online Coalition. Her previous work has a human rights-centered approach to technology, emphasising encryption, censorship, and cybersecurity. We have invited her to contribute this perspective to the sat com governance discussions to provide a complete picture.

The volume concludes with a reflective section by J. Kulesza, who thoughtfully considers the volume as a whole, consisting of contributions offering unique perspectives and showcasing the authors' diverse expertise and preferred methodological approaches. From theoretical frameworks to empirical studies, the chapters collectively enhance our understanding of the role of satellite broadband in global connectivity and underscore its importance in global power dynamics, especially those impacted by security and cybersecurity. This book aims to inform policy and governance of satellite broadband, ensuring it is utilized to connect the millions currently disconnected while addressing security and sustainability concerns. J. Kulesza highlights the significance of the interdisciplinary approaches taken by the contributors, noting how their varied backgrounds and methodologies enrich the discourse on satellite broadband. The reflective section emphasizes the critical need for robust policies that not only promote widespread access to satellite broadband but also safeguard against potential security threats and ensure the long-term sustainability of these technologies. By addressing these multifaceted issues, the book provides a comprehensive overview of the current state and future prospects of satellite broadband.

We hope this volume will serve as a valuable resource for a broad audience, including civil society, scholars, practitioners, and students, fostering further research and dialogue. The insights presented in this volume are intended to inspire innovative solutions and collaborative efforts to bridge the digital divide, enhance global connectivity, and navigate the complex landscape of security and cybersecurity in the realm of satellite broadband.

SECTION I

https://doi.org/10.18778/8331-719-9.04

Understanding Low Earth Orbit (LEO) Satellites and Policy Issues

Dan York[1]

Internet access from systems such as Starlink and OneWeb in low Earth orbit (LEO) is changing people's lives and enabling many more people to join the online world. How do LEO systems work and what are the intersections with policy work?

The Basics of Satellite Internet Access

We have been using satellites for communications since the 1960s. Until recent years, almost all of those satellites were in a "geostationary" (GEO) orbit[2] at around 36,000 km from the surface of the Earth. A special aspect of this orbit is that a satellite orbits the Earth at the same rate as the Earth rotates, and so the satellite appears to be "parked" over a specific spot on the Earth's surface. This makes it easy for interacting with the GEO satellite. You can simply point a satellite dish on the ground at the satellite's position and communication can begin.

A GEO satellite communication system used for Internet access involves three components:

- **Satellite —** The satellite located at a specific location in geosynchronous orbit.
- **Satellite dish —**Typically referred to as a "user terminal", this is the device on the ground that enables users to connect to the satellite. For a consumer, it might be connected to a WiFi access point or other similar system. For a larger company, it might be connected to that company's network.
- **Ground station —** A location on the ground typically with large dishes/antennas that connects out to the Internet.

1 Internet Society, United States.

2 Note that in UN and International Telecommunications Union (ITU) policy terminology, satellites in geosynchronous orbit are referenced as "GSO" satellites versus "GEO" satellites.

A user in a home connected to a GEO satellite would connect to their local WiFi network. Their Internet requests go from their local satellite dish up to the GEO satellite and back down to a ground station, where they then go out across the Internet. Responses follow the same path, coming back to the ground station, up to the satellite, and down to the user's local satellite dish. This is often called a "bent pipe" connection.

From a policy point of view, for a GEO satellite to provide Internet access in a country, the local regulators will need to approve:

- **Spectrum allocation**—the usage of appropriate frequencies for both the "uplink" from the user's equipment and the "downlink" from the satellite to the ground station.
- **Consumer equipment**—the "user terminal" (aka "satellite dish") must receive the appropriate consumer electronics permissions to be used in the country or region.
- **Ground station(s)**—the satellite operator must obtain "landing rights" to operate a ground station within a country.

Based on treaties and conventions within the International Telecommunications Union (ITU), this set of approvals must be done within each country in order for a GEO satellite provider to operate.

Additionally, because there are only so many locations ("slots") possible within the geosynchronous orbit of the earth, the ITU is responsible for regulating those locations. A satellite operator must get permission from the ITU before it can launch a satellite into a specific GEO location.

An advantage of GEO satellites is that because they are "parked" over a specific location on the Earth, many governments have invested in launching satellites that are located over their country and provide communication and Internet services to their country. Additionally, because they are so far from Earth and have such a large field of view of the planet, a company looking to provide global service can use as few as three GEO satellites to cover most of the world. GEO satellites also typically have a life expectancy of 15–20 years before they need replacement.

The Rise of LEOs

The fundamental challenge with using GEO satellites for Internet access is the enormous distance from the surface of the Earth. It can take a packet at least 600 milliseconds (ms) to travel from the Earth to a satellite and back—in some cases it can be even longer.

In a world in which we have become accustomed to online video calls and so many other forms of real-time communication, this amount of "latency" (sometimes called "lag") simply will not support the kind of communication we use every day. Most voice or video calls need less than 150 ms of latency to work. Similarly, modern use of online gaming, e-sports, virtual worlds/metaverse, high-speed

trading, and just regular messaging need to have significantly lower amounts of latency. A typical fiber or cable broadband connection can be more in the range of 10–50 ms of latency, and many Internet service providers (ISPs) are continually working to create even faster connections with lower latency.

The solution for faster, lower-latency satellite-based Internet is to move the satellites closer to Earth. Starting in the 1990s, multiple government and commercial organizations started looking at using satellites in Low Earth Orbit (LEO) below 2000 km from the Earth's surface and also Medium Earth Orbit (MEO) from 2,000–36,000 km (everything between LEO and GEO).[3]

A challenge with LEO satellites is that they orbit faster than the Earth's rotation, and so instead of just having one satellite "parked" above a location, you need to have 100's or 1,000's in order for a satellite dish to always have access.

The LEO systems in the 1990s from companies such as Teledesic, Iridium, and Globalstar were not commercially successful at that time but research continued. In the 2000s and 2010s new companies emerged including O3B, OneWeb, SpaceX. Ultimately it was the launch of SpaceX's Starlink in 2020 and 2021 that made people everywhere see the potential in high-speed, low-latency connectivity from LEO orbits.

The Difference with LEOs

As noted above, the major difference with LEO-based systems is that instead of a single GEO satellite or a small number of GEO satellites, a company operating a LEO system must launch a "constellation" of hundreds or thousands of satellites. Additionally, because the satellites are closer to the Earth, they are subject to more gravitational pull and atmospheric drag and therefore only have about a five-year lifespan. The operator of a LEO system must be prepared to be constantly launching new satellites to replace older ones.

As of August 2025, SpaceX has over 8,100 Starlink satellites in orbits ranging from around 450–550 km from Earth. Eutelsat has around 650 OneWeb satellites in orbits around 1,200 km. Multiple other LEO constellation operators are beginning to launch their satellites.

The satellite dishes for both the user and the ground station must also change. Unlike a GEO satellite where a dish can just be pointed at the location of a satellite and left alone, with a LEO constellation the dish must be constantly tracking multiple different satellites. Rather than physically moving a dish, systems such as Starlink or OneWeb use "electronically steerable"/"phased array" antennas where all the tracking of satellites is done electronically inside of the "dish".

3 In UN and ITU policy terminology, satellites in both LEO and MEO are referred to as "Non-geostationary" or "NGSO" satellites.

Similar to GEO systems, a LEO operator must engage with the regulators in *each* country to obtain spectrum allocations, consumer equipment approvals, and ground station landing rights.

Space Lasers

One challenge for LEO-based systems is the need to be in range of a ground station to connect down to the rest of the Internet. In the initial LEO deployments, this often meant having ground station located every 900 km or so, requiring a rather massive investment in setting up ground stations, with all the necessary government approvals.

A significant innovation with LEO-based systems has been the emergence of inter-satellite lasers (ISLs) connecting between satellites in a constellation. This allows the user to connect to a satellite and then have their traffic go across the "mesh" of the constellation until it gets to a satellite within range of a ground station.

This has enabled connectivity from remote locations such as Antarctica, and also from locations where for various economic or regulatory reasons it is challenging to locate a ground station.

SpaceX's Starlink constellation uses ISLs, and Amazon's Project Kuiper has indicated that they will use ISLs as well. Unfortunately due to the proprietary nature of these systems, not much is known about the capacity and other capabilities of these ISLs.

From a policy point-of-view, the potential use of ISLs has a couple of interesting aspects. On the positive side, ISLs potentially allow a country to quickly get started with Starlink without the investment in one or more ground stations. However, this can be a negative as some countries may use a ground station as a point for enforcement of national security or monitoring.

Deployment Challenge—Launching Rockets

As this article is being written in early 2025, the single largest barrier to deployment of satellites into LEO is not as much a regulatory issue as it a practical matter—there is only one company globally, SpaceX, that is consistently and reliably launching rockets at a pace necessary to operate a LEO constellation.

Given that LEO constellations need to have hundreds, if not thousands or even 10s of thousands, of satellites—and also that LEO satellites only have a lifespan of 5 years before they need to be replaced—LEO constellation operators need to be almost constantly launching new satellites.

Right now SpaceX is the only company continually launching rockets. In 2024 their Falcon 9 rocket was launched over 120 times, frequently carrying around 20 Starlink satellites, but also carrying satellites for other providers. SpaceX has also

been launching test flights of its massive Starship rocket which, when in production, is expected to carry possibly hundreds of satellites into LEO.

All of the other traditional launch providers are in a transition between their rockets and had very few launches. United Launch Alliance (ULA), a company formed by Boeing and Lockheed and historically the primary launch partner for NASA, is in the process of transitioning to their Vulcan Centaur rocket—and only had one launch in all of 2024. Similarly, Arianespace, the traditional launch partner for European companies and governments, is transitioning to the Ariane 6 rocket and only had one launch in 2024. Both companies are hoping for more in 2025, but they have a long way to go to catch up to the cadence of SpaceX.

The intense demand for launch services has created an entire ecosystem of new companies seeking to provide launch capacity. Blue Origin, a company from Amazon founder Jeff Bezos, has been seeking to launch its "New Glenn" rocket for several years now. Blue Origin finally succeeded in launching New Glenn in January 2025, but it's not clear how many launches will be possible in 2025. Many other startups have emerged seeking to provide launch services.

However, at this moment in time it is only SpaceX that is capable of consistently providing launch services, and as a result, deployment for other constellations beyond Starlink is waiting on availability from SpaceX for launching.

Policy Issues

Beyond the regulation aspects mentioned earlier, there are a wide range of policy issues around LEO-based systems, many of which will be addressed in other sections of this book. A quick summary includes:

- **Affordability—**Most LEO systems involve a significant up-front cost for the user terminal ("dish") and then a monthly subscription fee. For many parts of the world that need the connectivity the most, these systems are not affordable. In some areas new business models are emerging such as renting out Starlink equipment for a monthly fee. We are also seeing governments or businesses subsidizing the cost of the initial equipment.
- **Competition with terrestrial network operators—**One of the barriers for LEO operators obtaining regulatory approval to operate in a country or region is often the resistance by the existing ground-based network operators. Both mobile/wireless network providers and fixed broadband providers view LEO operators as a competitive threat and will push back using regulatory appeals, lobbying for legislation, or legal maneuvers to block the approvals. Often government officials will agree with the network operators and will seek some way to compensate local network operators.
- **Requirements around local economic participation—**Some regions also have requirements that Internet or telecom operators in a country must have some local economic participation. It could be the requirement to have an

office in the country. It could be that a certain percentage of economic activity must involve local companies. However, the LEO operators are by nature more of global ISPs, and particularly for the companies such as SpaceX that have a direct-to-consumer business model, there is very little need for engaging in the local economy.

- **Economic flow to global corporations**—Which points to the larger challenge that allowing LEO operators into a country means that the equipment and subscription fees will flow not to local companies but instead to global companies such as SpaceX, Eutelsat or Amazon. Most of these companies are based in the US or Europe which often adds another dimension to policy discussions.
- **Lack of competition**—As of early 2025, only SpaceX is operating a LEO constellation that is globally providing service. OneWeb has launched sufficient satellites and has begun offering Internet connectivity in some regions of the world, but is reportedly still struggling to line up all their required ground stations to achieve global connectivity. At this time there is very little competition for LEO-based connectivity. This may change over the years ahead, but we will see.
- **Security/monitoring**—For some countries it is important that there be some capacity for monitoring Internet traffic, potentially for blocking certain sites. This can be a challenge for LEO-based systems given that they are global ISPs, or it can at least introduce delays in regulatory approvals.
- **Spectrum wars**—There are only so many radio frequencies available for transmitting and receiving information. And "sharing" of a frequency is not always possible due to interference between systems. For this reason, radio frequency usage is standardized and regulated through the ITU's Radiocommunications Sector (ITU-R) and through national regulators. At this time there are many competing interests. For instance, some mobile network operators are seeking more frequency ranges for use for 5G or now 6G services. At the same time, LEO satellite operators are seeking more frequency ranges for various services. And the GEO operators are also seeking to ensure their systems are not subject to interference.
- **Technical issues around spectrum**—Some nations have discovered that they have interference issues that must be addressed before LEO systems can operate in their country. In some cases, the frequencies needed by SpaceX are already in use for government or military communication. As sharing can be challenging, and as the LEO satellites use common frequencies globally, the government must consider how it can move local communication to other frequencies so that the satellites can work.
- **Astronomy interference**—Another type of interference of great concern to the scientific community is the interference from the thousands of LEO satellites for both visual and radio measurements for astronomy and other related

research. It is not only the quantity of satellites, but also the size. For instance, the newest satellites from AST Space Mobile are expected to be 223 square meters with their antennas fully extended, which is about the size of half of a basketball court.

- **Space debris**—With LEO satellites only having about a 5-year lifespan, there is great concern about what happens when satellites reach their end-of-life. Will the satellites "de-orbit" correctly and burn up in the upper atmosphere? Separately, what happens if satellites collide or explode and create debris fields? There are efforts underway such as the Zero Debris Charter, but this remains an area of serious concern.[4]
- **Environmental and climate concerns**—Also of concern is what happens to the Earth's atmosphere as all of those satellites reach their end-of-life and burn up in the upper atmosphere. Will that be okay? Or will there be impacts to the upper atmosphere that will cause greater climate effects later on? There are many unknowns here as we collectively enter into this grand experiment of launching 10s of thousands of satellites into LEO.
- **Unproven long-term business model**—This 5-year lifespan also raises the question of how many of these LEO system providers will have a sustainable business model. A LEO operator must pretty much be continually launching new satellites to replace the ones that will be aging out. Hundreds or thousands of satellites will need to be manufactured—and then launched—each year. Will this business model work and be sustainable? We don't know.
- **Fragmentation**—Will all of these systems support the global public Internet? Or will some offer a different experience? Particularly as China launches LEO constellations, will this result in an extension of their restricted network?

All of these and many other policy issues are part of the discussions around this new form of space-based Internet access.[5]

Direct-to-Cell (DTC)/Direct to Device (DTD)

One specific new area for policy discussions is around direct communication between smartphones and satellites based in LEO. Until now, customers have needed to purchase a user terminal ("dish") that they used to connect to the LEO satellites for Internet access.

However, technology has advanced to where a regular smartphone can be used in what is being called "direct-to-cell (DTC)" or "direct-to-device (DTD)" connectivity. No need for dishes—you simply use your mobile phone.

---

4 European Space Agency, *The Zero Debris Charter*, Brussels 2025. Available at: https://www.esa.int/Space_Safety/Clean_Space/The_Zero_Debris_Charter (accessed: 25/02/2025).

5 For a longer discussion, see: Internet Society, *Perspectives on LEO Satellites. Using Low Earth Orbit Satellites for Internet Access*, Reston, Virginia, 2022. Available at: https://www.internetsociety.org/leos/ (accessed: 23/02/2025).

This capability is being heavily promoted by SpaceX and T-Mobile in the US as a result of a partnership agreement. In response, other US mobile companies such as AT&T and Verizon are looking to partner with another company named AST Space Mobile. In other parts of the world, local mobile companies are signing up to partner with SpaceX and other companies. Apple also has a long-standing relationship with Globalstar, one of the older LEO companies, for some forms of messaging connectivity.

Beyond the prolific marketing, the reality is that the DTC capabilities are still very limited right now. The systems work by having the LEO satellites equipped to transmit on frequencies used by mobile providers in addition to their regular satellite frequencies. By partnering with a local mobile provider, the LEO operator then gains permission to use those frequencies and can transmit and receive directly to and from smartphones. SpaceX has already sent over 400 satellites (of their 8,000+ satellites) into LEO with this capability. Other LEO operators such as AST Space Mobile are seeing this as their primary usage and are marketing themselves as essentially a "cell tower in space".

There are, however, serious technical challenges. All of us have been on a mobile phone when we've gone too far away from a cell tower and had the phone call fall apart and eventually drop. To communicate from space, satellites need larger antennas and different power levels. The substantial distance imposes very real challenges.

Today the systems are mostly limited to sending text messages, and usually only in a situation where no other connectivity is available. However, this offers tremendous capabilities for people to be able to reach someone wherever they may be.

The race is on now for LEO operators to be able to offer text messaging to smartphones, and then to go beyond that into voice calls and eventually Internet access. Some operators are exploring launching satellites into Very Low Earth Orbit (VLEO) below 400 km, which gets them closer to the ground and to users, but also requires more satellites and may impact the lifespan of the satellites. Other operators are looking at how to make satellites with larger antenna areas, which then introduce visibility and interference issues.

There are significant technical challenges, and the business models are not entirely clear, but there is great interest from both mobile operators and LEO operators in making this happen.

From a policy perspective, DTC opens *many* new issues. You now have transmissions to and from satellites on many different frequencies. You have the potential for global telecommunications companies, and you have competition issues with often only one mobile provider being able to partner with a LEO operator. There will be roaming, affordability, and economic issues – and so much more.

Regardless, this capability is well on its way and we are moving closer to a day when we all can potentially just use our smartphone from wherever we are on the planet.

Looking Ahead

The next few years are looking to be extremely busy for LEO. SpaceX is seeking to launch its full "Gen 2" constellation with potentially over 42,000 satellites. Eutelsat's OneWeb should begin global connectivity at some point soon. Amazon has begun launching their 3,000+ satellite Project Kuiper constellation in 2025. The European Union is looking to launch their IRIS2 constellation. The Canadian company Telesat has plans for a 1,500+ satellite Lightspeed constellation. AST Space Mobile is planning to launch 90+ of their massive satellites for smartphone connectivity.

Meanwhile, over in China, at least three different large LEO constellations are in the works. The Qianfan (Thousand Sails) constellation has launched over 70 satellites on their path to 14,000. The GuoWang constellation is being planned for 13,000 satellites, and another Honghu constellation is talking about 10,000 satellites.

Around the world, each week brings word of new startups that are planning to launch even more satellites into LEO. It's not clear how many of these constellations will actually successfully launch into space. Nor is it clear how many will be financially sustainable.

What is clear is that the next few years will be extremely busy for both technology and policy issues related to using Low Earth Orbit for Internet access. There is great potential for bringing truly life-changing connectivity to every location on the planet—IF we can accept the many challenges and tradeoffs.

Bibliography

European Space Agency (ESA), *The Zero Debris Charter*, Brussels 2025. Available at: https://www.esa.int/Space_Safety/Clean_Space/The_Zero_Debris_Charter (accessed: 25/02/2025).

Internet Society, *Perspectives on LEO Satellites: Using Low Earth Orbit Satellites for Internet Access*, Reston, Virginia 2022. Available at: https://www.internetsociety.org/leos/ (accessed: 23/02/2025).

https://doi.org/10.18778/8331-719-9.05

Historical Reflections & an Economic Approach to LEOs as Infrastructure

Jonathan Liebenau[1]

Introduction

This paper explains the context of the satellite industry from three related but distinct standpoints. These are presented in part 1, which is divided into sections addressing economics, then history and then business practices. Following that we will consider the relationship between digital infrastructure generally and satellite internet specifically. We start by addressing the basic economic question: who pays whom for what and under which circumstances? In a normal capitalist marketplace, the relationships among buyers and sellers, the state and public beneficiaries are all relatively clear. For digital infrastructures it is not very clear but for satellites it is even less clear for reasons that we will see.

The current convoluted set of relationships can best be understood from an historical perspective and so in the second part we will turn to the legacy we inherit and consider what the assumptions, expectations and behaviours of people, starting in around 1957–1958 with the International Geophysical Year, laid out the precedents that have become our legacy.[2]

In the third part we turn to the businesses themselves and their predecessors in government programmes that experimented with alternative business models. These conflicting revenue generating models offer us a baseline from which to

1 Department of Management, London School of Economics and Political Science (LSE), United Kingdom.

2 F.L. Korsmo, The genesis of the International Geophysical Year, *Physics Today*, 2007, 60(7), pp. 38–43. Available at: https://pubs.aip.org/physicstoday/article/60/7/38/686853/The-Genesis-of-the-International-Geophysical-Year (accessed: 20/12/2024).

compare variations in practice. We will see how satellites fit into the bigger picture of data infrastructure and how the economics of infrastructure allows us to discern specific trade-offs.[3]

The problem: *Cui bono* & who bears the cost?

Let's start with that fundamental question that bridges law and economics: *cui bono*? Before we can say anything about what the cost: benefit ratio might be, we need to have some idea of what the value of the network is, who ascribes value to it, and what relationship the value proposition holds to those who finance it. In the early history of infrastructure, systems were mostly private and faced competition, other than roads which have been mostly public for the past few hundred years. During the twentieth century most infrastructure elements became either sanctioned monopolies or public entities, sometimes through state owned enterprises, sometimes as public utilities, sometimes using other governance models. Only towards the late 20th century did liberalisation ideals begin to move more infrastructure towards private, competitive models. A landmark was the US AT&T telecommunications monopoly which was broken into competing elements starting in with an antitrust case filed by the US Justice Department in 1974 and culminating in the breakup of the system in 1984, followed by the privatization of British Telecom in the same year. Large swathes of other telecommunication, energy, water, transportation and other utilities in Britain and elsewhere were liberalized. The World Trade Organization and the European Union accelerated that trend in the early 2000s with the wholesale liberalization of telecommunications networks and services.

With early infrastructures, only small numbers of wealthy people could make use of what was on offer. The change occurred when it became clear to industrialized economies that the spillover effects of good quality, universal access was a major contributor to national economic growth. Infrastructure, in that sense, has been compared with, or even equated to, childhood education and, for the United States after 9-11, with the banking system which, when damaged, was re-labelled as "critical infrastructure" because its tight interconnectedness and massive spillover effects were newly recognized.

While we might wish to address the value question by measuring the benefits to individuals, to capture the logic of an infrastructure that offers cheap access and where extensive or universal service is required, we must consider what the spillover effects might be. This is not an easy measure to come to partly because infrastructure has become a foundation to the majority of

3 C. Giannopapa, A. Staveris-Poykalas, S. Metallinos, Space as an Enabler for Sustainable Digital Transformation: The New Space Race and Benefits for Newcomers, *Acta Astronautica*, 2022, 198, pp. 728–732. Available at: https://ui.adsabs.harvard.edu/abs/2022AcAau.198..728G/abstract (accessed: 20/12/2024).

economic activity, but economists try to measure, for example, how expensive a transport strike (or snow day shutdowns) are, or how much a big electricity outage costs to an economy. The resulting figures are very difficult to interpret and can hardly be directly used to address a question such as: how much would it be worth to re-build a system such as a smart energy grid.[4] Nevertheless, we need some kind of guide to help make decisions about things such as "how much can be spent to upgrade the broadband system", or "what is the cost of delaying the roll-out of 5-G for two years", or "what will the breakeven point be for a particular LEO constellation"?

The answer for LEOs cannot be limited to how many people use the system, or even how high a price the market can bear. The answer will have to come back to the spillover effects and some guess as to what the widespread economic benefits of the system might be over a relatively long period of time. We have an idea of what those spillover effects are, but it is much more difficult to measure them in aggregate, as opposed to recounting anecdotes, or "cases" which describe their effects. We have known since the 1980s that satellite telephony could provide polar explorers, isolated services providers and, of course, the military, with a valuable alternative. In those years the issue was less about the comparative costs of different infrastructures but rather the difference between access and no access, where building broadband (or ISDN) access would cost a few thousand dollars, compared with a few hundred dollars in fees for occasional hookup time.

For any investment the critical determinant of value is the timeframe in which the price can be amortized, the type of pay-off expected, and the date upon which the payoff is required.[5] Flaws in dealing with these simple dimensions of finance is sufficient to explain the failures of every preceding LEO project. For the current ones, the determinants might have more to do with the critical relationships between government engagement and private sector business models, in particular how procurement of services is going to be handled in the medium term, what the value of spin-offs might be for government users (military, surveillance, launch services, etc.), and what rules get applied for things such as taxation, subsidies, and crucially interconnection pricing.

---

4 We do try to think this through when we are asked whether a union's pay claim is reasonable or when we consider whether it is worth buying a whole lot of expensive snow removing equipment.

5 McKinzie estimated that initial cost for a LEO system is between $5–10 billion, that maintenance would run to $1–2 billion per year and that the components' lifespan is around five years. C. Daehnick et al., *Large LEO satellite constellations: Will it be different this time?*, McKinsey & Company, New York 2020. Available at: https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/large-leo-satellite-constellations-will-it-be-different-this-time (accessed: 20/12/2024).

How did we get here?

To place the current situation in the context of longer trends, let's look back to a perspective from the 1990s. We could go back even further, to the founding of Inmarsat in the mid 1970s, or even earlier to Sputnik, or even the 1920s imagining of satellites in what was largely the realm of science fiction. What characterized the image, the plans, and even the early commercial investments of the 1990s was a gamble on there being a market beyond both military and civil government buyers. There was also the reasonable hope that continued liberalization in countries such as the US and Britain would bring real markets into military services (such as lesser-secure communications and maybe a large part of GPS) and perhaps statutory functions such as property registries or land management for national parks and other government-owned estates.

Governments could certainly become real, lucrative markets, but the big money from the 1990s perspective was going to come from businesses such as mining companies, big agriculture, and transport/logistics (beyond what Inmarsat was doing). One example of this led to a study of the LEO industry in the late 1990s because the UK Civil Aviation Authority and their National Air Traffic Control Service needed to know whether and when LEOs would be reliable as well as financially feasible to integrate into their existing communications systems, or perhaps even supersede the legacy technologies.[6]

There were never a large number of companies involved, but enough to give a sense that most of the major problems were being addressed by firms not directly associated with governments. It was remarkable in retrospect in that there were no gazillionaires pouring their money and egos into the sector and it looked for a good long while that we were not heading towards any sort of monopoly, even if NASA was going to continue playing the anchor role.

Launch technologies were one broad area of exploration with quite successful trials of high-altitude airplane launches, plausible plans and trials of equator-based shipboard launchpads,[7] and a wide range of ideas about cheap designs and rocket fuels. There were investments in what we might call very-low stations, or very high-altitude communication equipment comparable to satellite technologies installed in drones and dirigibles, or even tethered balloons. Later both Google and Facebook, as well as various broadband companies, spent considerable sums on piloting such schemes.[8]

---

6 J. Liebenau, *The Economics and Business Models of LEOs with Regard to the Provision of Communication Services for Civil Aviation*, unpublished report, UK Civil Aviation Authority, London 1999.

7 Sea Launch, *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Sea_Launch (accessed: 20/12/2024).

8 T. Simonite, Alphabet and Facebook's Stratospheric Internet Plans Get Tangled in High-Altitude Red Tape, *MIT Technology Review*, 26 March 2016. Available at: https://www.technologyreview.

Small, very inexpensive satellites were being built at a commercial spinoff of Surrey University and sold to governmental and private land management, mineral exploration and other such organizations.[9] They had three simple ideas behind their business model: include only minimally necessary technologies, keep the whole package very small, and use as many off-the-shelf components as possible. This third idea was most intriguing because it required advanced engineering applied to product testing so that they could identify, for example, the very highest quality couple of batteries out of a large batch of apparently identical products. Prices were already low by the late 1990s around ten years after the founding of Surrey Satellite Technology Ltd. [SSTL], who knew that together with others developing low-price launch services they were headed to a scalable market. By the early 2000s they had launched and commercialized remote sensing services and the successful Disaster Monitoring Constellation.

Illusions about the company came to an end in 2004 for some when Elon Musk acquired a 10% stake[10] (and was awarded an honorary doctorate from the university) but four years later Airbus Industries, through EADS Astrium, took over. From that time on the SSTL served mainly their customers, including the Galileo system and more recently products such as S-Band Synthetic Aperture Radar to monitor suspicious shipping activity. It also produced an Active Debris Removal technology to de-orbit space stuff.

Surrey Satellite Technology Ltd during its first twenty years is but one example of potential business models for the satellite industry and as they were also leading researchers into constellation engineering, a model of how a relatively integrated LEOs business might have constituted a coherent supply chain as well as competed for private sector and governmental business. It was also apparent what the market niches were likely to be in sectors such as resources exploitation. As for telecommunications services the targets were all marginal: exploration and adventure, emergency services, special redundant lines of communication, and suchlike.

Perceived obstacles

So, what were the perceived obstacles? Three categories will both help explain the problem as of the early 2000s help to frame it for the second quarter of the 21st century. The first of these will always be scientific, not always in the sense

com/2016/03/26/71292/alphabet-and-facebooks-stratospheric-internet-plans-get-tangled-in-high-altitude-red-tape/ (accessed: 20/12/2024); M. Reynolds, Facebook and Google's race to connect the world is heating up, *Wired*, 26 July 2018. Available at: https://www.wired.com/story/google-project-loon-balloon-facebook-aquila-internet-africa/ (accessed: 20/12/2024).

9 Surrey Satellite Technology Ltd. Available at: https://www.sstl.co.uk/ (accessed: 20/12/2024).

10 SpaceNews, SpaceX Takes 10 Percent Stake in Surrey Satellite Technology, SpaceNews 2023. Available at: https://spacenews.com/space-x-takes-10-percent-stake-surrey-satellite-technology/ (accessed: 20/12/2024).

that there are insoluble problems but in the sense that our expectations are always on the rise. A few longstanding, large scale research themes have emerged that are either specific to LEOs, such as the mathematics and physics of constellation structures, or at the intersection of either telecommunications, such as spectrum management, or closely related technologies, such as theories associated with earth sensing problems.

The second area of obstacles is in the technical realm and continues to include now the hundred year old problems of rocket fuel and launching as well as the newer problems of controlling satellites and the perennial effort to extend miniaturisation. Reuse of rockets, from early space shuttle designs to recent reusable launch systems, fall into that category.

It is the third realm, that of policy, that will persist as the most troubling of the clusters of obstacles. Much of this will become a matter of law and public preference after various communities have expressed their opinions, shaped their norms, institutionalized them and moved toward legislation. However, before the bread and butter of satellite law can become routine for concerns such as business affairs, international dispute resolution and regulatory compliance, many problems need to be carefully considered so that jurisdiction can be clarified, social norms articulated and institutions appropriately shaped. Some of these were already on the minds of participants in International Geophysical Year discussions in 1957!

Early stakeholders

Before we turn to the current business models and their economic context, it is important to understand the earlier efforts to commercialize satellites both because there is much to learn from the ways in which choices were made in the period from the 1970s to the 2000s and because many of the practices and institutions of that era have become precedents for current organizations and activities.

I like to think of Inmarsat as a key predecessor in part because it had a recognizable relationship with both governmental and commercial interests and because its various iterations exemplify critical features that have been variously built into subsequent business models. Following the Convention on the International Maritime Satellite Organization (of the International Maritime Organization—IMO) in 1976, INMARSAT immediately launched three (now 15) geostationary satellites and became operational before the end of that decade.[11] What is remarkable is that from the outset its remit spanned governmental, inter-governmental and commercial governance. By the end of the 1990s it was privatized and after a spell on

11 *Convention on the International Maritime Satellite Organization*. Available at: https://www.imo.org/en/About/Conventions/Pages/Convention-on-the-International-Maritime-Satellite-Organization.aspx (accessed: 20/12/2024).

the stock market it was largely acquired by Harbinger Capital and then an investment consortium until more recently (2021) acquired by Viasat.[12]

The subsequent history of satellite companies should not be regarded as a simple linear progression as, in addition to the many dead ends and reverses, the broad foundation to the current set of business models is comprised of companies such as ORBCOMM, founded in the late 1980s, Globalstar in the early 1990s, and Iridium, in the late 1990s. European ventures, such as O3b, and others, such as the UAE Yahsat, were founded in the following decade. This early generation of satellite companies all suffered financial turbulence, going in and out of bankruptcy: ORBCOMM in 2000, Iridium in 2001, Globalstar and Teledesic both in 2002, etc. Clearly there were problems in the business models although the dot.com bust of 1999 and the larger telecoms financial crash of 2001–2004 directly contributed to the crisis of investor confidence.

What were those business and why were they all so flawed? The basic components of the business models were largely common although their structures were distinct as each sought a unique or at least competitive niche. They had in common an idea of strategic planning for digital access although their core customer base varied from governments to rural communities to maritime users to emergency and NGO organizations.

LEO business models

The locus of revenue generation, however differed and the choices made about where premium profits might accrue in relation to where cross subsidies might be used distinguished the companies and shaped their finances and sometimes their technologies. This is evident, for example, in the choices of LEO constellation configuration or indeed whether the satellites might be placed in a medium- or geostationary orbit. It is evident in what connections were made to maritime or aviation interests, civil governmental or military establishments.[13] The technical trade-offs may be somewhat clear, between high versus low latency configurations, between expensive, heavy, powerful payloads versus mini-satellites, between broad global coverage versus orbital geometries that allow services only for densely populated latitudes.

Starlink's initial intention, if Elon Musk's comments on opening in 2015 are to be believed, was that it would provide backhaul traffic and 'about 10% of local business and consumer [internet] traffic',[14] in high-density cities. It was soon estimat-

12 Viasat, *Viasat history*. Available at: https://www.viasat.com/about/who-we-are/viasat-history/ (accessed: 20/12/2024).

13 Bipartisan Policy Centre, *Overview of the Low Earth Orbit Satellite Industry.* Available at: https://bipartisanpolicy.org/leo-satellite-industry/ (accessed: 20/12/2024).

14 O. Cliff, SpaceX Seattle, *YouTube*, 2015. Available at: https://www.youtube.com/watch?v=A-HeZHyOnsm4 (accessed: 31/12/2024); *Starlink*, Wikipedia. Available at: https://en.wikipedia.org/wiki/Starlink (accessed: 20/12/2024).

ed to cost around $10 billion[15] and the US Federal Communication Commission offered and later revoked $885.5 million worth of federal subsidies to support rural broadband customers.[16] Nevertheless, revenues seem to have moved from eight years of losses to a small profit currently, based in large part on a little over 4 million subscribers.[17] These subscribers pay for broadband at various levels of service but there is also a business line for the US Space Development Agency for military and dual-use satellites but this may not continue as a major revenue stream given the preference shown for competitors York, Lockheed Martin and Northrop Grumman. Nevertheless, military applications for related businesses, especially Starshield,[18] are likely to continue to be closest to the core of the business model.

OneWeb has a very different business model and one primarily dependent on national satellite organizations, in particular that of the UK government, the regional, formerly intergovernmental organization now liberalized company, Eutelsat, and big investors including Bharti Global (of India) and Japan's SoftBank.[19] It has had satellites in orbit for little over 5 years and currently targets governments (including military users), large corporations and (isolated) communities rather than individual customers, as is core to the Starlink business model.

At the same time that OneWeb began to build its LEO constellation, Amazon established Kuiper in effect to compete more directly with Starlink. It began launching only late in 2023 and offers low-latency broadband connections at prices affordable to many individual consumers.[20]

The long-established SES (formerly Société Européenne des Satellites) is a publicly quoted company largely owned by the government of Luxemburg that is based on a different business model to provide telecommunications network

15 G. Shotwell, SpaceX's Plan to Fly You Across the Globe in 30 Minutes, *YouTube*, 14 May 2018. Available at: https://www.youtube.com/watch?v=Dar8P3r7GYA&t=591s (accessed: 20/12/2024).

16 U.S. House Committee on Oversight and Accountability, *Comer Probes FCC Decision to Revoke Starlink Funds*, 7 October 2024. Available at: https://oversight.house.gov/wp-content/uploads/2024/10/10.7.2024-Letter-to-the-FCC58.pdf; https://oversight.house.gov/release/comer-probes-fcc-decision-to-revoke-starlink-funds/#:~:text="In%202020%2C%20the%20FCC%20awarded,%2C%20video%20calls'%20and%20more (accessed: 20/12/2024).

17 Starlink, *X*, Available at: https://x.com/Starlink/status/1839424733198344617 (accessed: 20/12/2024).

18 Starshield, *SpaceX*. Available at: https://www.spacex.com/starshield/ (accessed: 31/12/2024); M. Sheetz, SpaceX Unveils 'Starshield,' a Military Variation of Starlink Satellites, *CNBC*, 5 December 2022. Available at: https://www.cnbc.com/2022/12/05/spacex-unveils-starshield-a-military-variation-of-starlink-satellites.html (accessed: 31/12/2024).

19 OneWeb, *Our story*. Available at: https://oneweb.net/about-us/our-story (accessed: 31/12/2024).

20 Amazon Staff, Amazon shares an update on Project Kuiper test satellites space launch: October 2023 update, *About Amazon*, 16 October 2023. Available at: https://www.aboutamazon.com/news/innovation-at-amazon/amazon-project-kuiper-test-satellites-space-launch-october-2023-update (accessed: 31/12/2024); T. Kohnstamm, Everything You Need to Know About Project Kuiper, Amazon's Satellite Broadband Network, *About Amazon*, 11 November 2024. Available at: https://www.aboutamazon.com/news/innovation-at-amazon/what-is-amazon-project-kuiper (accessed: 31/12/2024).

backhaul services for both leading economies and emerging economies, services for the hyperscalers [Amazon's] AWS and [Microsoft's] Azure, and a variety of other products such as platforms for digital broadcasting. Its broad customer base and network of medium-orbit as well as geostationary satellites puts it in a different competitive position. Unlike the leading LEO firms, SES grew substantially by acquisition and it backs, for example, O3b, along with Google and investors HSBC and some leading asset management companies.[21]

Data infrastructure and where LEOs fit

With an understanding of the basic economics and associated business models, we can focus on the character of the satellite business from the perspective of data infrastructure. The term and its synonyms such as e-infrastructure, digital infrastructure and information infrastructure has come to mean that underlying set of facilities, utilities and services that constitute the internet, very broadly defined, and the means to access it. We include in this of course the data centres, internet exchanges, hosting services, broadband networks and all the businesses that support or depend on them. Included are the vast network of undersea cables and of course the satellite constellations that provide connectivity.[22]

These are clearly associated with economic activity, but the relationship is not simple. That is because in some places sophisticated data infrastructure is a consequence of prosperity, in some cases it is a prerequisite for economic growth. In many places national economic policies are predicated on the assumption that it needs to be extended through investments; from local businesses, from government, from development agencies such as the World Bank, or from foreign direct investments by multinational companies.

However, just as we have seen the differences among the business models for LEO firms, there are many different ways in which the architecture of data infrastructures shape the markets and in particular determine the source of premium profits. For example, the condition as to whether the telephone/broadband network operator has access to high rents from household customers as opposed to those providing "over the top" services such as Netflix or Amazon Prime. Consider all the different players and their claims to premium profits: in some places

21 *SES Annual Report 2023*, SES Satellite, Luxemburg 2024. Available at: https://www.ses.com/sites/default/files/SES-Annual-Report-2023.pdf (accessed: 31/12/2024). See also: SES (Company), *Wikipedia*. Available at: https://en.wikipedia.org/wiki/SES_(company) (accessed: 31/12/2024) with links to industry reports about numerous acquisitions, documenting its growth strategy.

22 J. Liebenau, P. Karrberg, Modelling the Economic Impact of Cloud for Development: An Analysis of Banking, E-Commerce and Telecoms in Egypt, Indonesia, Kenya, Mexico, and Turkey, *Proceedings of the TPRC2024 – The Research Conference on Communications, Information and Internet Policy*, 2024. Available at: https://ssrn.com/abstract=4910699 (accessed: 31/12/2024).

payment systems are regarded as utility services, in some places they are a profit centre. In some places Google effectively charges local network operators for the opportunity to offer access to GMaps and Gmail to their customers, in other places it is the network operator who charges Google for the service they provide in carrying their internet traffic.

It is for this reason that numerous alternative business models have emerged for the satellite industry and that there are no set conditions for competition as yet. Just as with other aspects of data infrastructure, the key determinants are going to be who the target markets are—governments, corporations, individuals or other bodies—and their scale and willingness to pay. Crucially, it also depends on the patience of investors. This differentiates the deep pockets and long range strategic planning that the American technology giants can apply from smaller competitors who take considerable risks when seeking to finance their activities through debt. It also differentiates them from governments that may or may not be willing to tolerate spending that could take more than a decade to bear fruit.

Trade-offs and choices

At the end we come to the core economic problem which we can frame around the simplest definition of economics: the distribution of scarce resources. Its starting point is the determination of the costs in relation to the benefits of the system. We have seen the basic entry cost is on the order of $10 billion and the most common beneficiaries are either investors who expect to make profits through revenues or through sale of the business (entrepreneurial exit). The other kind of beneficiary would be those who can utilize satellites for a related purpose such as national governments who expect returns through economic growth, or the major commercial users of internet such as Amazon (with Kuiper) who benefit both by the infrastructure components for their AWS business and through extending internet access to more customers for their e-commerce businesses.

Over the past 30 years the cost has come down dramatically, first through the development of small, cheap satellites such as those from Surrey, then through dropping cost to launch and then to simple scale economies associated with significant growth. The targets for revenue have not changed in type very much but they have changed in scale since internet access has dramatically widened and even more significantly traffic has boomed. This has incentivised business models based on individual and small group access, on business and supply chain customers, and on governments.

At this point it is appropriate to remind ourselves that there is a balance that needs to be struck between commercial and national interests. This is both because the national interest will eventually determine the rules of the game but also because governments constitute a critical, and in some cases the dominant, source of revenue for the companies. This is rarely an easy circle to square if for no

other reason than that the time frames in which business and policy are made are usually radically different. National policies often prioritize very long term goals and are framed in terms of national growth, security and the preferences either of some authoritarian leadership or some interpretation of the popular will. Security in particular often prevails and a military goal of controlling information (or access to information) is sometimes sought at (almost) any cost.

In a close-to-ideal situation, that is, one with large amounts of available finance, a spread of options and alternative elements of infrastructure would be planned. There would also be judicious choices among short, medium and long-term development projects. We have come to the point that LEOs in particular are able to offer rapid infrastructure installation so long as the huge entry costs are met. This doesn't obviate the need, however, to resolve the conflicting interest and alternative incentives between state and private interests. So, we should return to the questions about who benefits from which elements or functionalities of satellite systems and what the costs are to whom for choices made.

The main determinant of who benefits most and which sacrifices are required at the national level is a function of the extent to which an economy is reliant on data. For this we can use an approximation of data intensity by sector. For example, clearly some sectors are entirely reliant on data and associated services, such as banking and finance, online services and entertainments, e-commerce, etc. Other sectors are reliant to some degree but not to as great an extent, such as education, mainstream retail, export and import reliant businesses, etc. Others are far less dependent on digitalization for their basic functioning, even if digital accounts and communication are commonplace. These include many of the primary sectors such as agriculture, mining and fisheries.[23] So, a country such as Britain which is heavily reliant on banking and finance, has a great deal to gain from advanced, widespread digitalization while a country largely reliant on small-scale farming and oil & gas. For Egypt, a country with a large, occasionally restive population and an authoritarian government, the priorities of the army prevail. So, where there are trade-offs necessary between, say, privacy and surveillance or between unincumbered international data exchange and internal control, the loss of economic advantages that occur from advanced data infrastructure is a small proportion of current GDP. For a country such as Poland, which has done so much to become integrated into the European Union over the past 20 years, lack of access to advanced data infrastructure would be a major disadvantage. That is both because part of its economic transition has been to shift towards more data intensive sectors and because the very mechanisms of EU integration are predicated on uses of data services for trade, administration and citizen engagement. Some countries sacrifice little by prioritizing uneconomic practices, others are effectively

23 F. Calvino et al., A Taxonomy of Digital Intensive Sectors, *OECD Science, Technology and Industry Working Papers*, 2018, 14. Available at: https://www.oecd-ilibrary.org/docserver/f404736a-en.pdf?expires=1732893402&id=id&accname=guest&checksum=6A35209425167ACD86501006F7FE6514 (accessed: 31/12/2024).

forestalling economic ambitions, while for others it is effectively unthinkable to lose any opportunities afforded by effective data infrastructure components.

This approach allows for a somewhat different way to calculate value and to assess *cui bono*. While it may not provide an overall deadweight cost to maintaining an authoritarian/military state, it can show what the drag is going to be when data infrastructure is not used, in terms of slower growth of e-commerce or lesser engagement in trade or even brain drain that results from lack of access to digital economy jobs. Policy processes that determine these choices differ and are not yet synchronized either internationally or even internally. It is a rare occurrence that domestic industrial policy is well connected with space policy, although the European Space Agency and functions such as GOVSATCOM do make some effort.[24] Such policies notwithstanding, the initial conflict at the core of our analysis of the economics of LEOs as infrastructure lies is the relationship between the public and the private realms.

Conclusions

Satellite law will have to deal with all those familiar categories of rights and responsibilities that any commercial litigation encounters. It will have to devise the means to resolve grievances that arise from damages in space, including space debris and the Kessler syndrome and those that arise from context specific technicalities such as spectrum interference. It will also have to resolve all those ambiguities anticipated in discussions during the International Geophysical Year about jurisdiction, property rights and requirements for international coordination. In addition, there are specific economic features that will lead to disputes about who has access to data infrastructure. Where an undersea cable offers potential connection to a landing site the decision to build an internet exchange and associated data centres might be regarded as a cost-benefit calculation. The initial investment is likely to be a billion dollars or more and that price can be assessed in terms of the overall short- or medium- term trend for a usage area.

The problem looks different for satellite usage. For a constellation owner the entry cost may be an order of magnitude greater than connecting to a cable. However, for a customer the initial cost of interconnection is far smaller. This may mean that people's attitude towards connectivity will be very different and they may turn to the law to press for their perceived rights to connectivity. It may also mean that advocates of specific civic interests such as privacy or empowerment, or of social concerns for environmental protection will turn to the courts to pursue their goals.

That is where the big picture of satellite law and economics will be revealed.

---

24 *Resolution on the European Space Policy*, European Space Agency (ESA), June 2007. Available at: https://esamultimedia.esa.int/multimedia/publications/BR-269/offline/download.pdf (accessed: 31/12/2024).

Bibliography

Amazon Staff, Amazon shares an update on Project Kuiper test satellites space launch: October 2023 update, *About Amazon*, 16 October 2023. Available at: https://www.aboutamazon.com/news/innovation-at-amazon/amazon-project-kuiper-test-satellites-space-launch-october-2023-update (accessed: 31/12/2024).

Bipartisan Policy Centre, *Overview of the Low Earth Orbit satellite industry*. Available at: https://bipartisanpolicy.org/leo-satellite-industry/ (accessed: 20/12/2024).

Calvino, F. et al., A taxonomy of digital intensive sectors, *OECD Science, Technology and Industry Working Papers*, 2018, 14. Available at: https://www.oecd-ilibrary.org/docserver/f404736a-en.pdf (accessed: 31/12/2024).

Cliff, O., SpaceX Seattle, *YouTube*, 2015. Available at: https://www.youtube.com/watch?v=AHeZHyOnsm4 (accessed: 31/12/2024).

Convention on the International Maritime Satellite Organization. Available at: https://www.imo.org/en/About/Conventions/Pages/Convention-on-the-International-Maritime-Satellite-Organization.aspx (accessed: 20/12/2024).

Daehnick, C. et al., *Large LEO satellite constellations: Will it be different this time?*,McKinsey & Company, New York 2020. Available at: https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/large-leo-satellite-constellations-will-it-be-different-this-time (accessed: 20/12/2024).

European Space Agency (ESA), *Resolution on the European Space Policy*, 2007, June. Available at: https://esamultimedia.esa.int/multimedia/publications/BR-269/offline/download.pdf (accessed: 31/12/2024).

Giannopapa, C., **Staveris-Poykalas, A., & Metallinos, S.**, Space as an enabler for sustainable digital transformation: The new space race and benefits for newcomers. *Acta Astronautica*, 2022, 198, pp. 728–732. Available at: https://ui.adsabs.harvard.edu/abs/2022AcAau.198..728G/abstract (accessed: 20/12/2024).

Kohnstamm, T., Everything you need to know about Project Kuiper, Amazon's satellite broadband network, *About Amazon*, 11 November 2024. Available at: https://www.aboutamazon.com/news/innovation-at-amazon/what-is-amazon-project-kuiper (accessed: 31/12/2024).

Korsmo, F.L., The genesis of the International Geophysical Year, *Physics Today*, 2007, 60(7), pp. 38–43.

Liebenau, J., *The economics and business models of LEOs with regard to the provision of communication services for civil aviation*. Unpublished report, UK Civil Aviation Authority, London 1999.

Liebenau, J., **Karrberg, P.**, Modelling the economic impact of cloud for development: An analysis of banking, e-commerce, and telecoms in Egypt, Indonesia, Kenya, Mexico, and Turkey 2024. *Proceedings of the TPRC2024—The Research Conference on Communications, Information and Internet Policy*. Available at: https://ssrn.com/abstract=4910699 (accessed: 31/12/2024).

OneWeb, *Our story*. Available at: https://oneweb.net/about-us/our-story (accessed: 31/12/2024).

Reynolds, M., Facebook and Google's race to connect the world is heating up, *Wired*, 26 July 2018. Available at: https://www.wired.com/story/google-project-loon-balloon-facebook-aquila-internet-africa/ (accessed: 20/12/2024).

Sea Launch, *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Sea_Launch (accessed: 20/12/2024).

SES Satellite, *SES Annual Report 2023*. Luxembourg 2024. Available at: https://www.ses.com/sites/default/files/SES-Annual-Report-2023.pdf (accessed: 31/12/2024).

SES (Company), *Wikipedia*. Available at: https://en.wikipedia.org/wiki/SES_(company) (accessed: 31/12/2024).

Sheetz, M., SpaceX unveils 'Starshield,' a military variation of Starlink satellites, *CNBC*, 5 December 2022. Available at: https://www.cnbc.com/2022/12/05/spacex-unveils-starshield-a-military-variation-of-starlink-satellites.html (accessed: 31/12/2024).

Shotwell, G., SpaceX's Plan to Fly You Across the Globe in 30 Minutes, *YouTube*, 14 May 2018. Available at: https://www.youtube.com/watch?v=Dar8P3r7G-YA&t=591s (accessed: 20/12/2024).

Simonite, T., Alphabet and Facebook's stratospheric internet plans get tangled in high-altitude red tape, *MIT Technology Review*, 26 March 2016. Available at: https://www.technologyreview.com/2016/03/26/71292/alphabet-and-facebooks-stratospheric-internet-plans-get-tangled-in-high-altitude-red-tape/ (accessed: 20/12/2024).

SpaceNews, SpaceX takes 10 percent stake in Surrey Satellite Technology, *SpaceNews*, 2023. Available at: https://spacenews.com/space-x-takes-10-percent-stake-surrey-satellite-technology/ (accessed: 20/12/2024).

SpaceX, *Starshield*. Available at: https://www.spacex.com/starshield/ (accessed: 31/12/2024).

Starlink, *Wikipedia*. Available at: https://en.wikipedia.org/wiki/Starlink# (accessed: 20/12/2024).

Starlink, *X*. Available at: https://x.com/Starlink/status/1839424733198344617 (accessed: 20/12/2024).

Surrey Satellite Technology Ltd. Available at: https://www.sstl.co.uk/ (accessed: 20/12/2024).

U.S. House Committee on Oversight and Accountability, *Comer probes FCC decision to revoke Starlink funds*, 7 October 2024. Available at: https://oversight.house.gov/wp-content/uploads/2024/10/10.7.2024-Letter-to-the-FCC58.pdf (accessed: 20/12/2024).

Viasat, *Viasat history*. Available at: https://www.viasat.com/about/who-we-are/viasat-history/ (accessed: 20/12/2024).

SECTION II

https://doi.org/10.18778/8331-719-9.06

Low Orbit Blues: The Noir in Cybersecurity

Roy Balleste[1]

You are one thousand miles above the surface of Delmak-O...
— Philip K. Dick[2]

A Prelude to Exploration

Human life is valuable. Whether short or long, it leaves an imprint on humanity's story. The implications of entering the vastness of space and the fabric of time stir profound reflections on existence and the essence of survival. The outcome of space exploration and long-duration missions underscores the notion that traveling through space and time could grant astronauts an expansive panorama of the cosmos, compelling them to grapple with the realization that confronting the future is far more complex than it initially appears. The challenge ahead reminds humanity of valuable lives against the rising horizon of technology expanding from our cislunar space into interstellar space. The future compels legal experts to consider the meaning of space exploration. This exploration means embarking on a journey that, in essence, shifts one's place within the continuum of time.[3] Entering the great expense of outer space focuses our immediate attention on the Low Earth Orbit (LEO). The LEO orbit encompasses Earth-centered orbits with an altitude of 1,200 miles (2,000 km) or less.[4] This orbit is considered near enough to Earth for convenient

1 Stetson University College of Law, Gulfport, Florida, United States.
2 P.K. Dick, *A Maze of Death,* First Mariner Books edition 2013, New York 1970, p. 22.
3 W. Grey, Troubles with Time Travel, *Philosophy,* 1999, 74(287), p. 57.
4 A. Bowman, *Commercial Space Frequently Asked Questions*, NASA, 7 April 2024. Available at: https://www.nasa.gov/humans-in-space/leo-economy-frequently-asked-questions/#:~:text=What%20is%20the%20LEO%20Economy,services%20this%20region%20of%20space (accessed: 31/12/2024).

transportation, communication, observation, and resupply. It also is the area where the International Space Station currently orbits and where many proposed future platforms will be located.[5] A more precise measure of this orbit involves examining the range of elevations beneath which satellites are unable to sustain their trajectory (80–100 km) and the altitude beyond which the level of the entrapped radiation belts complicates satellite operations (up to approximately 2,000 km).[6] The LEO space is a symbol of present and future economic growth, where national interests in research evolve in parallel with plans of deep space exploration led by the Artemis program.[7]

This fascinating orbital space is not without challenges. A sort of low orbit blues menaces the future success of commerce and peaceful use of outer space. The International Telecommunication Union (ITU) noted in 2021 that about 2.9 billion people around the world lack access to the Internet.[8] This scenario offers the private sector commercial opportunities to work on the construction of small satellite constellations to provide Internet access from LEO.[9] One great advantage of this LEO orbit is its close proximity to the Earth's surface, with almost no delay in data transmission.[10] While this is a sign of hope and human development, additional geopolitical factors foreshadow this expected progress. Objects in Low Earth Orbit have become integrated into the vast web of the internet, resulting in an expanded attack surface for potential hackers.[11] The hack or destruction of LEO satellites could represent a disruption of a vital communication network, foreshadowing unexpected legal dilemmas. This is profoundly important in various situations, from regular Internet users relying on LEO data to astronauts exploring deep space, where the availability of services is vital for commerce or even survival.

LEO satellites serve as vital conduits, facilitating data transmission from earth-based stations to spacecraft, venturing into the vastness of deep space. The effect arises from a vast array of antennas strategically positioned across the globe, spanning all seven continents, complemented by satellites orbiting in space, which collectively facilitate the transmission of radio waves.[12] "Astronauts and mission

5 *Ibidem*.

6 J.C. McDowell, The Low Earth Orbit Satellite Population and Impacts of the SpaceX Starlink Constellation, *The Astrophysical Journal Letters*, 2020, 892(2), p. 1.

7 A. Guzman, *What is the Commercial Low Earth Orbit Economy?*, NASA, 26 July 2023. Available at: https://www.nasa.gov/humans-in-space/commercial-space/what-is-the-commercial-low-earth-orbit-economy/ (accessed: 31/12/2024).

8 Ch. Suwijak, S. Li, Global Internet Access from the Low Earth Orbit: Legal Issues regarding Cybersecurity in Outer Space, *Journal of East Asia and International Law*, 2022, 15(1), p. 93.

9 *Ibidem*.

10 *Ibidem*.

11 M. Holmes, 10 Defining Moments in Cybersecurity and Satellite in 2023, *Via Satellite*, 22 January 2024. Available at: https://interactive.satellitetoday.com/via/january-february-2024/10-defining-moments-in-cybersecurity-and-satellite-in-2023 (accessed: 31/12/2024).

12 *How Do We Communicate with Spacecraft? We Asked a NASA Technologist: Episode 37*, NASA. Available at: https://www.nasa.gov/general/how-do-we-communicate-with-spacecraft-we-asked-a-nasa-technologist-episode-37/ (accessed: 31/12/2024).

controllers rely on this network to transmit messages and commands."[13] Spacecraft in orbit can communicate directly with ground stations on Earth only when they possess an unobstructed view of ground stations, an occurrence that is generally brief.[14] The feasibility of this endeavor is attributed to the existence of "tracking and data relay satellites," commonly referred to as TDRS.[15] "These satellites relay data from spacecraft to ground stations, allowing NASA to provide near-continuous global communications coverage to missions in low-Earth orbit."[16] The TDRS is an essential conduit for transmitting information, facilitating space-based research and exploration from its vantage point in geosynchronous orbit around our planet.[17] The satellite constellation guarantees an almost unbroken global communications network encompassing more than thirty-five LEO-orbiting spacecraft.[18] This useful technology may also have additional applications.

Consider, for example, a scenario of fourteen colonists traveling on their way to a habitable exoplanet. Philip K. Dick relates the story of fourteen colonists who travel to the planet *Delmak-O*.[19] Each of them is brought there with the promise of a new beginning.[20] Upon arrival, they attempt communication via satellite, however, the communication system fails, leaving the colonists without contact and unable to leave the planet.[21] Eventually, the situation spirals into chaos as more time passes.[22] These are the events depicted in Philip K. Dick's novel, *A Maze of Death*. While the exact condition of space explorers in the vastness of deep space will be revealed as time unfolds, the more significant challenge lies in the nature of human existence. These are some of the factors explored by the novel. Notions of space exploration will highlight the next fifty years when nations will increase their presence in space and endeavor to safeguard their infrastructure. This will require grappling with the legal complexities stemming from inherent cyber vulnerabilities associated with space exploration. In the same spirit, the use of outer space encompasses cyberspace with all its activities. The future of humanity and its expansion to off-world colonies are the inspiration that Philip K. Dick shares in his most famous novel, *Do Androids Dream of Electric Sheep?*[23] Most popularly known

13 *Ibidem*.
14 *Ibidem*.
15 *Ibidem*.
16 *Ibidem*.
17 *Tracking and Tada Relay Satellite (TDRS): Continuing the Critical Lifeline*, Goddard Space Flight Center, NASA. Available at: https://www.nasa.gov/wp-content/uploads/2022/04/tdrsfact-sheet_3.pdf (accessed: 31/12/2024).
18 *Ibidem*.
19 P.K. Dick, *op. cit.*
20 *Ibidem*, pp. 9–21.
21 *Ibidem*, pp. 48–59.
22 *Ibidem*.
23 D.E. Williams, Ideology as Dystopia: An Interpretation of 'Blade Runner', *Revue Internationale de Science Politique*, 1988, 9(4), p. 384 ["Ridley Scott's Blade Runner became first a 'cult' film, and then a national institution: it is one of only fifty films to be deposited in the Library

as the novel behind the motion picture *Blade Runner*, the visionary work is considered one of cinemas' most fascinating noir sci-fi stories.[24] Both, the book and the motion picture are concerned with the essence of humanity.[25] As humans enter the next space age, notions of technology may threaten or improve humanity's ability to develop a new age of discovery in outer space.

Matters of Law and Orbits

Planet Earth is in a galaxy like no other. From a distance, it may look like many others. The closest world with intelligent life—if any—is unknown. In between, there are millions of planets and thousands of potential exoplanets spreading across the galaxy. But life may be rare, for planets harboring life may be unique and hard to find in the universe. Yet, our existence's noble purpose is to explore new worlds. Occasionally, it is appropriate to take a moment to reflect on the past, if only to recognize the distance traveled and to contemplate the future. In the vast expanse of outer space, the concept of borders fades into irrelevance. Yet, as the legal field considers the LEO orbit, challenges surface to cast shadows over long-held notions, igniting uncertainties within the fabric of current realities. Simply said, technology is continuously developing. This is the technical progression of low-earth orbit communications. In terrestrial endeavors, those who venture into the cosmos will rely upon an intricate web of communication systems, including LEO satellites. For example, Starlink and Project Kuiper are deploying networks of LEO satellites to provide global connectivity to the Internet, especially to underserved or remote areas.[26] LEO satellites provide rapid, reliable communication, offering an ideal alternative for broadband Internet and cellular services.[27] These satellites present a pragmatic solution. Their orbit is ideally suited for the nascent phases of space exploration, the rigorous testing of satellites, and the essential training of astronauts.[28] The International Space Station (ISS) provides another LEO example by enabling sustained

---

of Congress, Washington DC, on the basis of its contribution to film culture"]. *See also* N. Wheale, Recognizing a 'Human-Thing': Cyborgs, Robots and Replicants in Philip K. Dick's 'Do Androids Dream of Electric Sheep?' and Ridley Scott's 'Blade Runner,' *Critical Survey*, 1991, 3(3), pp. 297–304.

24 B. Sherlock, Blade Runner: 10 Tropes Of Film Noir (& How It Puts A Sci-Fi Twist On Them), *Screenrant*, 22 August 2020. Available at: https://screenrant.com/blade-runner-film-noir-tropes-sci-fi-twist/ (accessed: 31/12/2024).

25 *Ibidem*.

26 L. Press, Amazon Project Kuiper vs SpaceX Starlink, *CircleID*, 19 January 2024. Available at: https://circleid.com/posts/20240119-amazon-project-kuiper-vs-spacex-starlink (accessed: 31/12/2024).

27 How will LEO satellites change wireless business models?, *Real Wireless*, 21 August 2024. Available at: https://real-wireless.com/how-will-leo-satellites-change-wireless-business-models/ (accessed: 31/12/2024).

28 A. Bowman, *op. cit*.

human presence in space and advancing technologies that may serve explorers in the vastness of deep space.[29] In this context, the legal inquiry necessitates clarifying the threats of failed communications relays that connect LEO satellites. Addressing this inescapable cyber threat necessitates the realization that an analysis of cybersecurity law and policy incorporates the consideration of cyberspace prioritized.

The evaluation of the present challenge must include the possibility of an external malicious actor disrupting satellite systems. Professor Carl Christol, an esteemed authority on space law, emphasized the imperative for a renewed dedication to the rule of law in global matters aimed at fulfilling the aspirations of humanity.[30] He seemed concerned with the rule of law significantly shaped by a progressive and pertinent legal framework governing the space environment and its natural resources, which aimed at fulfilling humanity's aspirations.[31] Accordingly, to effectively tackle illicit activities threatening LEO satellites, stakeholders must recognize that human endeavors shape cybersecurity in outer space. As the threat environment expands to include interconnected domains, stakeholders should be prepared to deal with increased vulnerabilities. Christol further noted that evolving an international legal framework governing outer space will undoubtedly enhance the thrill of uncovering an innovative model of human experiences and interactions.[32] The challenge here involves individuals acting alone or directed by rogue nations to interfere with space missions through cyber means. This state of affairs, grounded in reality, resides within a partial legal void. As legal experts search for the rule of law, there is a point of departure. Article I, paragraph 2 of the Outer Space Treaty, notes that:

> Outer space, including the Moon and other celestial bodies, shall be free for exploration and use by all States, without discrimination of any kind, on a basis of equality and in accordance with international law, and there shall be free access to all areas of celestial bodies.[33]

The spirit of the Outer Space Treaty must be contrasted with the realities of rising global conflicts. Satellite technology exists for use in space, where their military capability may be exploited for reconnaissance, guiding weapons, and supporting other warfare activities on the surface of the Earth.[34] The nature of the utilization of

29 *Ibidem*.

30 C.Q. Christol, *Space Law: Past, Present, and Future*, Kluwer Law and Taxation Publishers, Deventer 1991, p. 495.

31 *Ibidem*.

32 *Ibidem*.

33 United Nations, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205, article II (entered into force 10 October 1967) [Outer Space Treaty].

34 R. Hagen, J. Scheffran, *International Space Law and Space Security. Expectations and Criteria for a Sustainable and Peaceful Use of Outer Space*, [in:] M. Benkö, K.-U. Schrogl (eds.), *Current Problems and Perspectives for Future Regulation*, Eleven International Publishing, AJ, Utrecht: The Netherlands 2005, p. 273.

space is tied directly to the activities of States, as Michel Bourély, former legal adviser to the European Space Agency, observed how space activities have emerged within the domain of nations, whether exclusively, as noted in certain cases, or in a more limited fashion, as seen in others.[35] Without a doubt, States have kept the primary control over those space activities that belong to the military.[36] But then again, military activities are linked to State sovereignty and, thus, the defense of the nation.[37] Along this line of reasoning, the rapid expansion of space-based systems to support military operations among the major powers has been observed. These activities have translated into real events, with "significant resources now devoted by each of them to the development of ever-more effective (and potent) space-related weaponry."[38] Sadly, the "prospect of a celestial war can no longer be regarded as mere fantasy."[39] In light of the legally ambiguous cyber threat landscape and the quest for meaning in a hostile environment, the noir in cybersecurity demands new guidance to delineate the future rule of law.

If humanity is to expand its exploration of the solar system and travel more frequently, its technology must be dependable. Yet, the concept of a nation engaging in cyber operations to disrupt the space infrastructure of another nation is more concerning, mainly if the nation permits the use of its territory for such operations.[40] The intersection of the cyber and space domains challenges all principles of space law and even all notions of international law. Michel Bourély also observed that operations conducted in outer space have a moral aspect that necessitates the rapid development of legal frameworks.[41] In the same vein, Bourély would agree that cyber activities in space are linked to state sovereignty. In other words, exploring outer space generally rests with responsible States.[42] While this concept is usually understood, it takes on a new meaning when cyberspace enters the analysis. Modern plans for the Moon and Mars should involve a forward-thinking approach, focusing on informed decision-making and risk reduction. The space industry should strive to be proactive rather than reactive to ensure a successful transition. And these proactive measures pose an intriguing question. Considering the challenge, it is essential to approach the analysis in a way that broadens the perspective of strategic threat intelligence for space activities. This approach should involve applying strategic thinking to the various factors in developing the LEO

35 M. Bourély, The Institutional Framework of Space Activities in Outer Space, *Journal of Space Law*, 1998, 26(1), p. 1.

36 *Ibidem*.

37 *Ibidem*, at 5.

38 J. Maogoto, S. Freeland, The Final Frontier: The Laws of Armed Conflict and Space Warfare, *Conn J Int'l L*, 2007, 23:1, p. 165.

39 *Ibidem*, p. 169.

40 D.E. Sanger, K. Conger, *Russia Was Behind Cyberattack in Run-Up to Ukraine War, Investigation Finds*, The New York Times, 10 May 2022. Available at: https://www.nytimes.com/2022/05/10/us/politics/russia-cyberattack-ukraine-war.html (accessed: 31/12/2024).

41 M. Bourély, *op. cit.*, p. 5.

42 *Ibidem*.

orbit. In the space industry, the process of intelligence gathering and understanding may begin with strategic threat intelligence. Thus, strategic threat intelligence is high-level knowledge of the global danger environment and an organization's role.[43] Strategic threat intelligence informs CEOs and other executives about cyber threats.[44] The research suggests that as traditional armed conflict becomes more risky and costly, cyberattacks are becoming increasingly attractive in the space between peace and full-scale war.[45] In this context, cyber operations emerge as an additional information security concern that can potentially extend to the far frontiers of space exploration.[46] These cyber operations have a specific goal, but their unpredictability can be intensified by additional disruptions that affect targets beyond the initial objective.[47]

While the space industry seeks solutions to new problems, Judge Manfred Lachs' advice acts as a guidepost.[48] It is thrilling to think of the other planets that await discovery and exploration. On such planets, colonists will arrive in one-way rockets, as in the case of *Delmak-O*, to participate in mystifying colonization programs.[49] Madred Lachs, former judge and president of the International Court of Justice, said that modern science's greatest feats are but a small part of a far larger epic.[50] In the same way, this approach could be considered the search for a strategic threat intelligence that seeks to avoid misjudging the threat actors and aims to discover informed business decisions.[51] Strategic threat intelligence may help LEO operations reduce cyber risks and better use existing data, which should lead to the development of laws that will manage the intricacies of the space domain. As the twenty-first century draws to a close, the LEO orbit may be poised to become increasingly congested with an array of satellites, space stations, and privately operated installations. The orbital lanes could stand on the precipice of chaos, where antiquated treaties provide inadequate protection against the encroaching influence of corporations, hackers, and rogue nations. The aspirations for peaceful exploration of the cosmos stand in stark contrast to the looming specter of armaments in the vastness of space. As the quest for power in the cosmos intensifies, nations engage in fierce competition to engineer anti-satellite weapons (ASATs)

43 IBM, What is threat intelligence? Available at: https://www.ibm.com/topics/threat-intelligence (accessed: 31/12/2024).

44 *Ibidem*.

45 J. Collier, Proxy Actors in the Cyber Domain: Implications for State Strategy, *St Antony's International Review*, 2017, 13(1), pp. 25–47.

46 D. E. Sanger, K. Conger, *op. cit.*

47 *Ibidem*.

48 M. Lachs, Thoughts on Science, Technology and World Law, *The American Journal of International Law*, 1992, 86(4), pp. 673–699.

49 P. K. Dick, *op. cit.*, p. 1.

50 M. Lachs, *op. cit.*, 45 at p. 677.

51 K. Barker, What is Cyber Threat Intelligence?, *CrowdStrike*, 23 March 2023. Available at: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/ (accessed: 31/12/2024).

designed to destroy orbiting satellites.[52] A distinct arena of anti-satellite technology that has recently garnered attention is the non-kinetic variant. Cyberattacks exemplify a remarkable form of non-kinetic anti-satellite strategies, harboring the capacity to cause significant damage to satellites.[53] A confrontation in space may very well extend beyond the confines of the LEO orbit. The existence of humanity, much like in any other sphere of endeavor, would find itself in peril. As time passes, it becomes increasingly apparent that an environment of rising tensions prevails.

One central consideration is the use of law as a tool for achieving a global order of human dignity, including the many aspects that this endeavor entails. Space industry stakeholders must search for legal norms that will offer certainty and promote the security of future space missions. The search for legal and technical standards does not respond to preordained theories or beliefs, instead, it is the response to tangible dynamics of cyber operations, their relations with governments, and their relevance to national security. The integration of cyberspace in the enhancement of space endeavors ought to be steered by the values of the Outer Space Treaty and the foundational tenets of relevant space law. Article I (2) of the Outer Space Treaty highlights the free exploration and use of outer space without discrimination of any kind.[54] While the expectation is that the use and exploration of outer space will be peaceful, the stakeholders must also acknowledge the rising threats and emerging attacks. The problem with assessing LEO orbit endeavors from the lens of space law, or even cyber law, is that it assumes that rules of behavior will be followed or that these rules are clearly defined and accepted. However, even for experts, the principles of behavior being drafted seem to "walk" carefully around geopolitics. However, the application of the rule of law to space operations should coincide with Article III of the Outer Space Treaty. This provision requires that space activities shall be conducted "in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international co-operation and understanding."[55] The task is to seamlessly integrate new cyber activities into evolving LEO endeavors.

The third decade of the twenty-first century is now emerging, and the US Space Operations Command has assigned cybersecurity and intelligence specialists to work with satellite operators to support military units and protect US systems with adequate cyber defenses.[56] US Admiral Michael Rogers, commander of US Cyber

52 M. Smith, Anti-satellite weapons: History, types and purpose, *Space*, 10 August 2022. Available at: https://www.space.com/anti-satellite-weapons-asats (accessed: 31/12/2024).

53 *Ibidem*.

54 Outer Space Treaty, *op. cit*.

55 *Ibidem*.

56 S. Erwin, Space Force shifting resources to intelligence and cybersecurity, *Space News*, 19 September 2022. Available at: https://spacenews.com/space-force-shifting-resources-to-intelligence-and-cybersecurity/ (accessed: 31/12/2024).

Command and director of the National Security Agency, once observed: "The seas around the world are, much like the cyber domain, not governed by one single nation."[57] He noted that humans needed to establish standards of conduct in the online world to maintain the free flow of knowledge and ideas, as had been done in the ocean.[58] It is now clear that a new and unified strategy is required to address the risks impacting space-enabled communications and associated human activities.

Dystopian Landscape

In 1958, Myers McDougal, a renowned international law scholar, warned that the conquest of space had barely begun.[59] His observations no doubt aroused interesting questions and encouraged further discussion. As if McDougal had a crystal ball to forecast the future, he anticipated a legal evolution necessitating the recognition of future difficulties, stressing the terrestrial basis of much of our law and the earthly methods in which, for some time, we would continue to think about law in outer space.[60] Today, as plans are drafted for the future, the inescapable truth lies within the human condition. McDougal correctly foresaw the increase in counterspace activities, which involve combining offensive and defensive operations to gain and sustain control and security in space.[61] To ensure the enduring essence of the Outer Space Treaty, security concerns must take precedence in any proposed plan. However, space law is failing to keep pace with the increasing number of objects being launched, the related cyber activities, and even the forthcoming astronaut missions.[62] This task presents a multitude of dangers that loom over humanity's progress as it seeks to explore the solar system. One of these threats emanates from the cyber domain.

The present state of cyberspace evokes images of a dystopian future where crime is rampant and law enforcement struggles to maintain order. This notion is clearly illustrated by the 1979 film *Mad Max*, released in the US by American International Pictures LLC/ Filmways.[63] This Australian dystopian action film tells the

57 M.S. Rogers, *Admiral, Address at the International Conference on Cyber Conflict*, NATO Cooperative Cyber Defense Centre of Excellence, Tallinn 2015.

58 *Ibidem*.

59 M.S. McDougal, Perspectives for A Law of Outer Space, *American Journal of International Law*, 1958, 52, pp. 407–431.

60 *Ibidem*.

61 Doctrine, Counterspace Operations, *Air Force Doctrine Publication 3–14*, LeMay Center for Doctrine Development and Education, United States Air Force, 1 April 2025. Available at: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-14/3-14-D05-SPACE-Counterspace-Ops.pdf (accessed: 01/04/2025).

62 See generally: R. Balleste, Cyber Conflicts in Outer Space: Lessons from SCADA Cybersecurity, *Emory Corporate Governance and Accountability Review*, 2021, 8(1).

63 B. Eggert, Mad Max, *Deep Focus Review*, 9 May 2015. Available at: https://www.deepfocusreview.com/reviews/mad-max/ (accessed: 31/12/2024).

story of a world with a declining rule of law.[64] Like the lawless hackers of present cyberspace, in the story, unbound motorcycle gangs roam the countryside.[65] The challenges of a lawless domain of human activity are illustrated by the efforts of the Australian Main Force Patrol (MFP) and their high-speed interceptors.[66] The story serves as an allegory for the present efforts of governments seeking to catch up to the hackers that race unbound across cyberspace. Whether with interceptors or computers, technology has been an excellent tool for improving the overall quality of human existence. It is the existence of humanity that defines behavior. In this setting, many cybercrimes may be considered traditional or "real world" crimes.[67] The borderless nature of cyberspace provides anonymity and a fertile environment to quickly impact victims globally.[68] This nature also makes it difficult to pinpoint a crime's origin. Given the disadvantages associated with forensic analysis, the time invested in attributing these activities is seen as a waste of time.[69] There is an additional drawback when dealing with criminals who exploit rapidly evolving technology to outsmart the government.[70] The intersection of technology and law highlights the glaring gap between legal frameworks and technological advancements, resulting in a pressing concern for public safety.[71]

Regrettably, a dystopian scenario is increasingly becoming a reality. Lately, there has been considerable discussion and study regarding the future of cyberspace and its impact on society. The Center for Strategic and International Studies conducted an analysis focused on warfare in cyberspace as part of their series "On Future War."[72] An innovative combination of public polls, expert forecasts, and AI-generated threat scenarios was employed to examine the evolving nature of cyber operations aimed at the United States.[73] The data is especially relevant because the study included a public survey of over 1,000 people from around the US and six tabletop

64 *Ibidem*.
65 *Ibidem*.
66 *Ibidem*.
67 K.M. Finklea, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction. Issues Confronting U.S. Law Enforcement,* Congressional Research Service 2013, p. 5.
68 *Ibidem*.
69 K. Zurkus, What's the Value in Attack Attribution?, *CSO Online*, 2017. Available at: https://www.csoonline.com/article/560371/is-identifying-an-attacker-a-waste-of-time.html (accessed: 31/12/2024).
70 K.M. Finklea, *op. cit.*, p. 18.
71 J.B. Comey, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*, Federal Bureau of Investigation, Washington 2014. Available at: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (accessed: 31/12/2024).
72 Y. Atalan, J.M. Macias, B. Jensen, *Eroding Trust in Government: What Games, Surveys, and Scenarios Reveal about Alternative Cyber Futures*, Center for Strategic and International Studies 2024, p. 2. Available at: https://www.csis.org/analysis/eroding-trust-government-what-games-surveys-and-scenarios-reveal-about-alternative-cyber (accessed: 31/12/2024).
73 *Ibidem*.

exercises with more than 50 top cyber specialists and experts in foreign policy.[74] The findings unveiled a projection of a cyber future characterized by targeted assaults on governmental services, essential infrastructure, and public confidence.[75] The findings also emphasize the tendency of potential adversaries to undermine the United States by means of cyberattacks that result in extensive disruption in critical services and small companies, along with espionage operations aimed at pillaging patents.[76]

The technical advancements over the last two decades have transformed into obstacles and drawbacks to overcome. In the US, for example, as criminals deliberately use new methods to commit the same crimes, the government, in contrast, finds itself in a defensive position when addressing illegal actions.[77] Sophisticated criminals can elude law enforcement due to their utilization of advanced technology and techniques that surpass the capabilities and knowledge of the government.[78] The utilization of advanced encryption to facilitate unlawful ventures exemplifies the challenge law enforcement faces in keeping pace with criminals.[79] The Department of Justice, Homeland Security, and numerous international organizations have identified impediments to assisting foreign governments in improving their ability to combat cybercrime.[80] Some significant drawbacks include a lack of specialized tools such as money, trained personnel, and a clear understanding of what constitutes a computer crime.[81] The cyberlandscape is mired by barriers stemming from the activities of hackers and similar actors, especially those engaged in malicious activities across national borders.[82] Cyber operations have become an easy tool of choice since these can be conducted anywhere in the world simply by accessing a computer and an Internet connection.[83]

The need for cybersecurity extends to satellite operations, which rely on a trio of interconnected segments. The US National Institute of Standards and Technology (NIST) defines the commercial space operations architecture as including space, ground, and user segments.[84] The *space segment* includes two parts. The first is the vehicle or satellite, which "consists of the platform and one or more

74 *Ibidem*.
75 *Ibidem*.
76 *Ibidem*.
77 K.M. Finklea, *op. cit.*, p. 18.
78 *Ibidem*.
79 *Ibidem*, p. 19.
80 Global Cybercrime, *Federal Agency Efforts to Address International Partners' Capacity to Combat Crime*, United States Government Accountability Office, Washington 2023. Available at: https://www.gao.gov/assets/gao-23-104768.pdf (accessed: 31/12/2024).
81 *Ibidem*.
82 I. Couzigou, Securing Cyber space: the Obligation of States to Prevent Harmful International Cyber operations, *International Review of Law, Computers & Technology*, 2018, 32(1), pp. 37–57.
83 *Ibidem*.
84 M. Scholl, T. Suloway, *Introduction to Cybersecurity for Commercial Satellite Operations*, National Institute of Standards and Technology, U.S. Department of Commerce, Washington 2023, p. 4.

payloads."[85] The second is the bus, which "consists of the components of the vehicle associated with the 'flying of the satellite,' such as power, structure, attitude control system, processing and command control, and telemetry."[86] Usually, the bus and the payload together comprise the satellite.[87] This space segment connects to the ground segment and user segment. The ground segment is comprised of ground operations (terrestrially-based) "that can be automated or conducted by human operators."[88] Lastly, the user segment includes the "consumers, such as Global Positioning Systems (GPS) receivers, satellite phone users, satellite Television receivers, vehicles, 5G users, industrial systems, mobile devices, and aircraft."[89] The US NIST has noted the associated threat to commercial space operations architectures, emphasizing the synergy of segments functioning as a cohesive whole.[90] Conversely, the realm of space communication represents a quintessential human endeavor, fraught with its own set of security challenges.

Nowadays, criminal behavior has taken root in cyberspace, which is both a complicated information highway and an arena for warfare. New laws are needed in every area where humans engage in activities, including on land, in the air, in space, and online. In other words, tackling the dangers of the cyber domain requires that scholars acknowledge that cybersecurity is at the core of human space activities. Information networks require practices and strategies to safeguard and defend them in an evolving new space arena. The core of information protection is reflected in *availability, integrity, and confidentiality*.[91] It involves an organization's overall risk assessment and considers law, due diligence, due care, and related risk management strategies. Indeed, an analysis of threats and challenges in the space industry from 1977 to 2019 reveals a broad attack surface.[92] The aforementioned discoveries, accessible in the public sphere, were classified according to the specific segment of space that was targeted, whether it was governmental, commercial, civilian, or military in nature.[93] Additionally, the incidents were classified based on the type of occurrence, such as jamming, spoofing, computer network exploitation, and hijacking.[94] The motivations behind these events were

85 *Ibidem*.
86 *Ibidem*.
87 *Ibidem*.
88 *Ibidem*, p. 6.
89 *Ibidem*.
90 *Ibidem*, p. 4.
91 J. Cawthra, M. Ekstrom, L. Lusty, J. Sexton, J. Sweetnam, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, NIST Special Publication 1800-25, U.S. Department of Commerce, Washington 2020. Available at: https://www.nccoe.nist.gov/publication/1800-25/index.html (accessed: 31/12/2024).
92 M. Manulis, C. Bridges, R. Harrison, V. Sekar, A. Davis, Cyber security in New Space: Analysis of threats, key enabling technologies and challenges, *International Journal of Information Security*, 2021, 20, pp. 287–311.
93 *Ibidem*, p. 295.
94 *Ibidem*.

also identified, including State espionage, hack and leak operations, and illicit activities.[95] Space cybersecurity researchers would not be surprised to know that the ground segment was the most targeted segment from the events analyzed, followed by RF data transmission.[96] Experts predicted this outcome due to attackers' experience with ground-based tactics and the worldwide reach of RF communications.[97] The painful realization is that space objects have been on hackers' list of targets. The study revealed that, in spite of operational o challenges, the space industry remains vulnerable to attacks, with eight documented cases, with most of those attacks—91%—targeting government-owned assets.[98] This happens against the background of the Outer Space Treaty, Article II, which asserts that the space domain "is not subject to national appropriation by claim of sovereignty."[99] This statement is one of the cornerstones of international space law and supports the true spirit enshrined in Article I (2), emphasizing that outer space is accessible for exploration and use without any restrictions. In the same manner, Article 45(1) of the International Telecommunication Union (ITU) Constitution specifies that the functioning of all stations must be conducted in a manner that does not result in detrimental interference with "radio services or communications."[100] Unfortunately, the existing norms for cyber operations are inadequate and more troublesome when applied to the space domain.

The Russian war of aggression in Ukraine has been paradoxical against the backdrop of the global rule of law. The current situation has resulted in an environment lacking in law and order as the strength of the rule of law diminishes. Within this environment, military offensive operations are carried out in accordance with the legal and policy frameworks established by governments. Retired US Army Lieutenant Colonel J.W. Shipp, a cybersecurity expert, acknowledges that cyberspace and outer space are global arenas for military operations, where the objective is to achieve supremacy to gain control over information.[101] According to Shipp, the essential objective in every domain is to ensure allies' actions and, if necessary, prevent enemies from acting.[102] He suggests that common elements can be used to devise a strategy.[103] In this regard, Article IV of the Outer Space Treaty, notes in relevant part, as follows:

95 *Ibidem*.
96 *Ibidem*.
97 *Ibidem*.
98 *Ibidem*.
99 Outer Space Treaty, *op. cit.*
100 *Constitution and Convention of the International Telecommunication Union*, 22 December 1992, 1825 UNTS 330, ATS (1994) 28, BTS 24 (1996) (entered into force date 1 July 1994), as amended by the 2018 Plenipotentiary Conference [ITU Constitution].
101 J.W. Shipp, Space and Cyberspace: The Overlap and Intersection of Two Frontiers, *Army Space Journal*, 2011, 10(1), pp. 40–41.
102 *Ibidem.*
103 *Ibidem*.

> The moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes. The establishment of military bases, installations, and fortifications, the testing of any type of weapons, and the conduct of military maneuvers on celestial bodies shall be forbidden.[104]

On the other hand, a dystopian landscape is unfolding, where rising power competition among nations is highlighted by various hackers, such as mercenaries, privateers, and spies, who bid to advance diverse agendas.[105] The Outer Space Treaty appears to be on a path toward obsolescence, with some of its provisions no longer able to guide the development of new technologies. In the cyberspace domain, legal developments are equally troubling. While various government experts have considered the operative aspects of these hackers or cyber operations for over ten years, discussions have focused on aspirational or soft law principles that suggest a voluntary honor code. This honor code-in-formation or international cyber norms began to evolve with the 2013 Report of the UN Group of Governmental Experts on Information and Telecommunications in the Context of International Security.[106] In 2021, the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security presented their report, observing that "efforts should be conducted in accordance with their obligations under the Charter of the United Nations and other international law, with a view to preserving an open, secure, stable, accessible and peaceful ICT environment."[107] The GGE, in the same 2021 report, paragraph 71(g) notes in particular the following:

> The Group reaffirms that States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. It also reaffirms that States must not use proxies to commit internationally wrongful acts using ICTs and should seek to ensure that their territory is not used by non-state actors to commit such acts.[108]

The efforts of the various UN Group of Governmental Experts considered the international community's expectations in search of norms for responsible state behavior. While these endeavors provide potential models for future guidelines or

104 Outer Space Treaty, *op. cit.*

105 *See generally*, T. Maurer, *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge University Press, Cambridge 2018.

106 United Nations, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98, 2013.

107 United Nations, Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security, UN Doc A/76/135, 14 July 2021, paragraph 18.

108 *Ibidem*.

codes of behavior, unfortunately, these are still ambitious and have not yet been fully realized. Therefore, other factors indicate the need for an alternative course of action. The world is more dangerous now than in the last decades of the twentieth century. In this tumultuous environment, due care continues to be crucial in launching best practices to protect organizations.[109] Given the offensive capabilities of hackers, terrorist groups, and criminal organizations engaged in transnational hostile cyber operations, stakeholders in the space sector have a vital responsibility to fulfill. It is imperative that they assume a proactive stance, exploring innovative avenues to confront these pressing cyber threats. In the grand tapestry of the cosmos, the true essence of peaceful exploration lies in the harmonious collaboration of nations and the collective spirit of humanity.

Gray-Zone Power

The concept of cyberspace has undergone significant development, expanding beyond its original scope of basic accessibility to encompass a multifaceted domain of human interactions and activities. The data sources driving humanity's progress have become essential to an intricate network of activities supporting the private sector, governments, and individual users. Human behavior is intricately linked to the pursuit of solutions and the addressing of illicit conduct in order to strengthen national and international justice.[110] The human perception of justice seems inherently consistent over many geographical locations and historical periods.[111] Accordingly, to effectively tackle illicit activities in cyberspace, stakeholders must recognize that human endeavors shape cybersecurity. Human action does not occur alone; instead, it is influenced by broader cultural ideas.[112] Familiarity with the thought process involved in combat is equally necessary for defense.[113] Similarly, understanding the cultural context helps to clarify the goals of policymaking and planning.[114] As the threat environment expands to include interconnected domains, stakeholders must prepare to deal with increased vulnerabilities.

The 2007 Estonian Distributed Denial of Service (DDoS) attack prompted cybersecurity experts to recognize the rapid evolution of cyberspace, as well as the

109 M. Whitman, H. Mattord, *Management of Information Security*, Cengage Learning, Boston 2016, p. 231.

110 D. Sznycer, C. Patrick, Intuitions about justice are a consistent part of human nature across cultures and millennia, *The Conversation*, 21 October 2022. Available at: https://theconversation.com/intuitions-about-justice-are-a-consistent-part-of-human-nature-across-cultures-and-millennia-190523 (accessed: 31/12/2024).

111 *Ibidem*.

112 R.E. Guadagno, A. Lankford, N.L. Muscanell, B.M. Okdie, D.M. McCallum, Social Influence in the Online Recruitment of Terrorists and Terrorist Sympathizers: Implications for Social Psychology Research, *Revue Internationale de Psychologie Sociale*, 2010, 23(1), pp. 25–56.

113 *Ibidem*.

114 *Ibidem*.

adaptation of traditional techniques to novel contexts. A novel cybersecurity threat emerged, causing a redefinition of covert transnational operations.[115] Consequently, the attack demonstrated the potential for disabling vulnerable systems, which could have severe consequences for a nation and its citizens.[116] This attack, which disregarded the rule of law, has been replicated multiple times since 2007. Ironically, the DDoS assault in Estonia likely laid the foundation, at least partially, for the current state of cyberspace.[117] Experts studying Russia's capabilities have observed that satellite-based systems might be a possible target.[118] This scenario is not too far-fetched, considering the hostile actions witnessed in Estonia that gradually intensified over the subsequent years.[119] The situation reached a tipping point in 2015, when Russian hackers carried out a significant cyberattack on an electric grid, targeting three power companies in Ukraine.[120] After the invasion of Ukraine, Russia launched variants of the wiper data destruction malware against Ukrainian targets.[121] It would have been a reasonable assumption to expect Russia to expand its cyber operations into space. The VIASAT case of 2022 became a cautionary tale of cyber operations that now intersect space services. However, to fully understand the lessons, it is necessary first to consider other factors.

From the beginning of the Russian invasion of Ukraine in 2022, Ukrainians experienced the effects of an assortment of cyber operations that included the deployment of multiple variations of malware—wipers—to destroy data.[122] This escalated with the Russian VIASAT-Skylogic breach, which revealed the existing susceptibility of a space network to exploitation by any actor with relevant technical skills.[123] Unfortunately, the criminal element lurking in cyberspace blurs the borderlines for law enforcement across jurisdictions.[124] Although national boundaries serve local, state, and federal jurisdictions, they also affect criminal activity and law enforcement operations.[125] Due to their transnational nature and wide-ranging consequences, these attacks should not be addressed solely through any State's efforts, no matter how powerful. Thus, it is imperative for stakeholders to acknowledge the 2022 Viasat KA-SAT Satellite hack as a clear indication of

115 G. Evron, Battling botnets and Online Mobs. Estonia's Defense Efforts During the Internet War, *Georgetown Journal of International Affairs*, 2008, 9(1), pp. 121–126.
116 *Ibidem*.
117 *Ibidem*.
118 S. Bendett, M. Boulègue, R. Connolly et al., *Advanced military technology in Russia. Capabilities and Implications*, Chatham House, Royal Institute of International Affairs, London 2021, p. 35.
119 *Ibidem*.
120 *Ibidem*.
121 M. Kaminska, J. Shires, M. Smeets, *Cyber Operations During the 2022 Russian Invasion of Ukraine. Lessons Learned (so far)*. European Cyber Conflict Research Initiative, Leiden 2022, p. 4.
122 *Ibidem*.
123 M. Manulis et al., *op. cit.*, p. 297.
124 K.M. Finklea, *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction. Issues Confronting U.S. Law Enforcement*, Congressional Research Service, Washington 2013.
125 *Ibidem*.

Russia's intensifying cyber operations interfering with the space domain. It is notable that several States have this capability.

A journey to the Moon, Mars, and other celestial bodies encompasses thoughts of optimism, high hopes, and a future-oriented perspective infused by human activity. Yet, if we are to look into the proverbial "crystal ball," the future shows satellite constellations, the Lunar Gateway, and increased crewed missions expanding human presence in the space landscape. If humanity is to achieve that success, then two realities must be recognized above all others. First, the nations of the planet, especially the spacefaring nations, must work together toward that common goal. Humanity as a whole must recognize how, in the event of a significant conflict involving major nations with space capabilities, the orbital region of Earth would be positioned to serve as a potential theater of warfare.[126] Second, while laws give guidelines that must be carried out under rule-governed direction, no legislation can ever ensure its honest implementation. [127] Indeed, the Outer Space Treaty has been in force for almost sixty years, yet, at present, a simple update of that treaty cannot be realized, even when the space law community recognizes the need for an update. Why does this idle status prevail? The truth is that the existing legal framework in cyberspace is more of a suggestion than an enforceable legal standard, and this status is slowly poisoning the activities of humanity in outer space. Other factors, such as mining for resources, and the race for the Moon and Mars, have increased competition among nations. As the conflict in Ukraine has demonstrated, a single factor is clear: the rule of law has no authority over transborder cyber operations, even when a space service is involved. Recognizing the gravity of space operations requires facing the truth: international cooperation is painfully slow and, at the moment, nonexistent.[128] The existing *legal lacunae*, better exemplified as *gray-zone conflict,* complicates matters. The gray-zone conflict is characterized by activities of subterfuge or malice utilized by States and non-State actors to "exploit gaps and ambiguities in the law."[129] Technology has made the gray-zone conflict more common and its effect more widespread.[130] This is supported by empirical data that shows how non-State actors use information technology to harm targeted infrastructure.[131]

The current landscape of activities is also profoundly influenced by the dynamics of the *great power competition*, a framework that elucidates the nature of global,

126 B.E. Bowen, *War in Space. Strategy, Spacepower, Geopolitics*, Edinburgh University Press, Edinburgh 2022, p. 281.

127 J.L. Esposito, *Law and Morality: A Survey of Ideas, Issues, and Cases*, Ethics International Press, West Yorkshire 2022, p. 12.

128 B. Ramsey, An Ethical Decision-Making Tool for Offensive Cyberspace Operations, *Air & Space Power Journal*, 2018, 32(3), p. 63.

129 R. Brooks, *Rule of Law in the Gray Zone*. Modern War Institute, 2 July 2018. Available at: https://mwi.westpoint.edu/rule-law-gray-zone/ (accessed: 31/12/2024).

130 *Ibidem*.

131 *Ibidem*.

interstate interactions shaped by political pursuits throughout history, culminating in the era preceding World War II.[132] Over time, numerous competition periods have seen strong national powers contend for prestige and prominence.[133] While the competition was limited to a two-state competition between the US and the USSR, it has resurfaced in international relations and security studies recently, due to globalization and American supremacy.[134] It has been noted how the US National Security Strategy of 2017 openly advanced the notion that the United States, Russia, China, and other national powers had formally transitioned from collaboration to competition.[135] The problem arises from the continuum of relations between governments, nonstate actors, and specific super-empowered individuals, ranging from cooperation to confrontation, ultimately culminating in warfare.[136] In the current era of global power dynamics, the shift towards a competitive-dominant engaging framework among the most influential nations and others has introduced greater conflict and confrontation into the realm of competition.[137] This scenario has led to heightened readiness for possible conflicts, encompassing advancements in antisatellite technology and exceeding all that has been witnessed in the recent past.[138]

The advancement of a solution necessitates an understanding of the purpose behind the technology that aids humanity's objectives and consciousness. The intricate tapestry of contemporary technology presents a complex challenge in the pursuit of a universal framework for human dignity. In an age where humanity finds itself intricately woven into a vast tapestry of connectivity, a paradox emerges: the stakeholders face an array of novel threats that seek to undermine their inherent dignity. This situation necessitates the establishment of a novel framework for space law. Myers MacDougal and Florentino Panlilio Feliciano, Associate Justice of the Supreme Court of the Philippines, noted how the rapid diffusion of weapons capable of shattering the globe, the hostile polarization of power in the world arena, the ever more precarious equilibrium between national actors, and many other aspects magnify with chilling insistence, even for the willful blind, the urgent need for rational inquiry into the inherited principles for controlling violence between peoples.[139] Indeed, should the inhabitants of Earth continue to find themselves in conflict, the prospects for the future appear bleak, fraught with tension, and shrouded in ambiguity.

---

132 T.F. Lynch III, *Introduction*, [in:] T.F. Lynch III (ed.), *Strategic Assessment 2020: Into a New Era of Great Power Competition*. Institute for National Strategic Studies, NDU Press, Washington 2020, p. 1.

133 *Ibidem*.

134 *Ibidem*.

135 *Ibidem*.

136 *Ibidem*, p. 2.

137 *Ibidem*, p. 3.

138 *Ibidem*.

139 M.S. McDougal, F.P. Feliciano, International Coercion and World Public Order: The General Principles of the Law of War, *Yale Law Journal*, 1958, 67(5), p. 771.

So, how should the space industry proceed? The solution resides in the steadfast adherence to the principles of law and order. The pursuit of space exploration serves as a mirror to the myriad activities of humanity. In the boundless expanse of the universe, human endeavors will transcend our wildest imaginings, unfolding in ways we have yet to comprehend. Thus, the inherent virtues of humanity, coupled with the principles of space law, shall ignite a renaissance of exploration beyond our terrestrial confines. If humanity must enter a new age of discovery, incorporating the entire solar system into its new domain, then "[a] more *substantive* concept of the rule of law [should] aspire to fill the idea of the law with notions of substantive justice."[140] Justice must illuminate the endeavors of those embarking upon this new era of exploration, for it is impossible to overlook the escalating demands, unmatched in their breadth and intricacy, for the expansion of sovereign authority.[141] In a similar vein, this observation extends to the vast cosmic ocean and the principles governing its exploration. The principles and regulations governing the Low Earth Orbit are of particular significance. Striking a balance between essential order and inevitable chaos means achieving a common point of reference and a tool to protect the world. The direction of threat intelligence depends much on this. The current state of space cybersecurity evolves from valuable lessons originating in past knowledge based on security strategy, legal principles, and industry standards. However, this knowledge must be intended for risk assessments, security requirements, and an innovative space law. While an argument can be made that new norms in international law are emerging and applicable to cyberspace and its intersection with the space domain, the same can be said of the existing grey area surrounding that law.

Beyond the Horizon: Conclusion

The future of space exploration is one of hope and awe. Due to the complexities of present geopolitics, the need to explore outer space in search of new worlds seems far removed from the trivialities of human existence. The future of humanity holds the potential for interstellar space travel. These tasks are theoretically possible, albeit costly and challenging from the current perspective. The noir in cybersecurity, however, is simply a disappointment with the current state of the law at the intersection of cyberspace and outer space. This noir is literal pessimism. "Film noir is a stylized genre of film marked by pessimism, fatalism, and cynicism. The term was originally used in France after WWII, to describe American thriller or detective films in the 1940s and 50s."[142] To encapsulate the essence of noir, space

140 S. Wiessner, The Rule of Law: Prolegomena, *Zeitschrift für deutsches und amerikanisches Recht*, 2018, 82, p. 83.

141 *Ibidem*.

142 *What is Film Noir? A Brief History with Examples from Cinema*, Studiobinder, 27 June 2021. Available at: https://www.studiobinder.com/blog/what-is-film-noir/ (accessed: 31/12/2024).

industry stakeholders must acknowledge the intricate web of satellite communication, coupled with the shortcomings of existing regulations, underscoring the urgent necessity for a cohesive framework of principles.

"Noir stories typically feature gritty urban settings, morally compromised protagonists, dark mysteries, and a bleak outlook on human nature."[143] Will humanity find and settle in *Delmak-O* or similar exoplanets? Astronauts and relevant stakeholders will surely face dangers after they land on the Moon and travel on to Mars. The process begins with the LEO orbit. Such guidelines are essential to safeguarding data as it traverses the vast expanse between Earth, satellites, and the cosmos.[144] "Launch servicing companies, remote sensing companies, and data access and analytics firms all share a desire to capitalize on the development and growth primarily in LEO satellites."[145]

In this landscape, cyber operations emerge as another information security risk that touches the spirit of human space exploration.[146] Utilizing cyber threat intelligence, which facilitates gathering, examining, and distributing data to identify, monitor, and predict possibilities and risks within cyberspace, enhances decision-making.[147] By leveraging threat intelligence, stakeholders gain a valuable perspective on the ever-evolving landscape of threats, vulnerabilities, and tactics malicious actors employ.[148] The noir in cybersecurity encourages new practices, standards, and norms to help secure the space industry. The attractive promise of providing global internet access via LEO satellite constellations is expected to generate around $400 billion in growth for the space sector by 2040.[149] Observing the landscape of the next twenty years, and even one hundred years, offers a beginning that traces its wisdom into the past and evolves into the future. The path to a workable space cybersecurity framework that ensures defensive capabilities in LEO can be developed from the wisdom of those scholars who long ago identified the benefits of space exploration, recognizing that peace and security evolve from uncertainty. The immediate solutions are contained in a new cybersecurity framework that, anchored in space law, will inspire the development of novel legal principles.

---

143 *What Is Noir Fiction?*, MasterClass, 27 Jan 2022. Available at: https://www.masterclass.com/articles/noir-fiction (accessed: 31/12/2024).

144 *Ibidem*.

145 A. Saboorian, A Brave New World: Using the Outer Space Treaty to Design International Data Protection Standards for Low- Earth Orbit Satellite Operators, *Journal of Air Law and Commerce*, 2019, 84(4), pp. 575–604, 580.

146 D.E. Sanger, K. Conger, *op. cit.*

147 J. Kotsias, A. Ahmad, R. Scheepers, Adopting and Integrating Cyber-threat Intelligence in a Commercial Organization, *European Journal of Information Systems*, 2022, 31(1), p. 35.

148 Shweta, K. Aditham, M. Hoeper, *What Is Threat Intelligence? Definition, Types & Process*, Forbes Advisor, 12 October 2023. Available at: https://www.forbes.com/advisor/business/what-is-threat-intelligence/ (accessed: 31/12/2024).

149 A. Saboorian, *op. cit.*, p. 582.

Bibliography

Atalan, Y., **Macias J.M.**, **Jensen B.**, *Eroding Trust in Government: What Games, Surveys, and Scenarios Reveal about Alternative Cyber Futures*, Center for Strategic and International Studies 2024. Available at: https://www.csis.org/analysis/eroding-trust-government-what-games-surveys-and-scenarios-reveal-about-alternative-cyber (accessed: 31/12/2024).

Balleste, R., Cyber Conflicts in Outer Space: Lessons from SCADA Cybersecurity, *Emory Corporate Governance and Accountability Review*, 2021, 8(1).

Barker, K., What is Cyber Threat Intelligence?, *CrowdStrike*, 23 March 2023. Available at: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/ (accessed: 31/12/2024).

Bendett, S., **Boulègue, M.**, **Connolly, R. et al.**, *Advanced military technology in Russia. Capabilities and Implications*, Chatham House, Royal Institute of International Affairs, London 2021.

Bourély, M., The Institutional Framework of Space Activities in Outer Space, *Journal of Space Law*, 1998, 26(1).

Bowen, E., *War in Space. Strategy, Spacepower, Geopolitics*, Edinburgh University Press, Edinburgh 2022.

Bowman, A., *Commercial Space Frequently Asked Questions*, NASA, 7 April 2024. Available at: https://www.nasa.gov/humans-in-space/leo-economy-frequently-asked-questions/#:~:text=What%20is%20the%20LEO%20Economy,services%20this%20region%20of%20space (accessed: 31/12/2024).

Brooks, R., *Rule of Law in the Gray Zone*. Modern War Institute, 2 July 2018. Available at: https://mwi.westpoint.edu/rule-law-gray-zone/ (accessed: 31/12/2024).

Cawthra, J., **Ekstrom, M.**, **Lusty, L.**, **Sexton, J.**, **Sweetnam, J.**, *Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events*, NIST Special Publication 1800-25, U.S. Department of Commerce, Washington 2020. Available at: https://www.nccoe.nist.gov/publication/1800-25/index.html (accessed: 31/12/2024).

Christol, Q.A., *Space Law: Past, Present, and Future*, Kluwer Law and Taxation Publishers, Deventer 1991.

Collier, J., Proxy Actors in the Cyber Domain: Implications for State Strategy, *St Antony's International Review*, 2017, 13(1), pp. 25–47.

Comey, J.B., *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*, Federal Bureau of Investigation, Washington 2014. Available at: https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course (accessed: 31/12/2024).

Constitution and Convention of the International Telecommunication Union, 22 December 1992, 1825 UNTS 330, ATS (1994) 28, BTS 24 (1996) (entered into force date 1 July 1994), as amended by the 2018 Plenipotentiary Conference [ITU Constitution].

Couzigou, I., Securing Cyber space: the Obligation of States to Prevent Harmful International Cyber operations, *International Review of Law, Computers & Technology*, 2018, 32(1), pp. 37–57.

Dick, P.K., *A Maze of Death*, First Mariner Books edition 2013, New York 1970.

Doctrine, Counterspace Operations, *Air Force Doctrine Publication 3–14*, LeMay Center for Doctrine Development and Education, United States Air Force, 1 April 2025. Available at: https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-14/3-14-D05-SPACE-Counterspace-Ops.pdf (accessed: 01/04/2025).

Eggert, A., Mad Max, *Deep Focus Review*, 9 May 2015. Available at: https://www.deepfocusreview.com/reviews/mad-max/ (accessed: 31/12/2024).

Erwin, S., Space Force shifting resources to intelligence and cybersecurity, *Space News*, 19 September 2022.

Esposito, J.L., *Law and Morality: A Survey of Ideas, Issues, and Cases*, Ethics International Press, West Yorkshire 2022.

Evron, A., Battling botnets and Online Mobs. Estonia's Defense Efforts During the Internet War, *Georgetown Journal of International Affairs*, 2008, 9(1), pp. 121–126.

Finklea, K.M., *The Interplay of Borders, Turf, Cyberspace, and Jurisdiction. Issues Confronting U.S. Law Enforcement*, Congressional Research Service 2013.

Global Cybercrime, *Federal Agency Efforts to Address International Partners' Capacity to Combat Crime*, United States Government Accountability Office, Washington 2023. Available at: https://www.gao.gov/assets/gao-23-104768.pdf (accessed: 31/12/2024).

Grey, W., Troubles with Time Travel, *Philosophy*, 1999, 74(287).

Guadagno, R.E., **Lankford, A.**, **Muscanell, N.L.**, **Okdie, B.M.**, **McCallum, D.M.**, Social Influence in the Online Recruitment of Terrorists and Terrorist Sympathizers: Implications for Social Psychology Research, *Revue Internationale de Psychologie Sociale*, 2010, 23(1), pp. 25–56.

Guzman, A., *What is the Commercial Low Earth Orbit Economy?*, NASA, 26 July 2023.

Hagen, R., **Scheffran, J.**, *International Space Law and Space Security. Expectations and Criteria for a Sustainable and Peaceful Use of Outer Space*, [in:] M. Benkö, K.-U. Schrogl (eds.), *Current Problems and Perspectives for Future Regulation*, Eleven International Publishing, AJ Utrecht, The Netherlands 2005.

Holmes, M., 10 Defining Moments in Cybersecurity and Satellite in 2023, *Via Satellite*, 22 January 2024.

How Do We Communicate with Spacecraft? We Asked a NASA Technologist: Episode 37, NASA. Available at: https://www.nasa.gov/general/how-do-we-communicate-with-spacecraft-we-asked-a-nasa-technologist-episode-37/ (accessed: 31/12/2024).

IBM, *What is threat intelligence?*Available at: https://www.ibm.com/topics/threat-intelligence (accessed: 31/12/2024).

Kaminska, M., **Shires, J.**, **Smeets, M.**, *Cyber Operations During the 2022 Russian Invasion of Ukraine. Lessons Learned (so far)*, European Cyber Conflict Research Initiative, Leiden 2022.

Kotsias, J., **Ahmad, A.**, **Scheepers, R.**, Adopting and Integrating Cyber-threat Intelligence in a Commercial Organization, *European Journal of Information Systems*, 2022, 31(1), pp. 35–51.

Lachs, M., Thoughts on Science, Technology and World Law, *The American Journal of International Law*, 1992, 86(4), pp. 673–699.

Lynch III, T.F., *Introduction*, [in:] T. F. Lynch III (ed.), *Strategic Assessment 2020: Into a New Era of Great Power Competition*, Institute for National Strategic Studies, NDU Press, Washington 2020.

Manulis, M., **Bridges, C.**, **Harrison, R.**, **Sekar, V.**, **Davis, A.**, Cyber security in New Space: Analysis of threats, key enabling technologies and challenges, *International Journal of Information Security*, 2021, 20, pp. 287–311.

Maogoto, J., **Freeland, S.**, The Final Frontier: The Laws of Armed Conflict and Space Warfare, *Conn J Int'l L*, 2007, 23:1.

Maurer, T., *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge University Press, Cambridge 2018.

McDougal, M.S., Perspectives for A Law of Outer Space, *American Journal of International Law*, 1958, 52, pp. 407–431.

McDougal, M.S., **Feliciano, F.P.**, International Coercion and World Public Order: The General Principles of the Law of War, *Yale Law Journal*, 1958, 67(5).

McDowell, J.C., The Low Earth Orbit Satellite Population and Impacts of the SpaceX Starlink Constellation, *The Astrophysical Journal Letters*, 2020, 892(2).

Press, L., Amazon Project Kuiper vs SpaceX Starlink, *CircleID*, 19 January 2024. Available at: https://circleid.com/posts/20240119-amazon-project-kuiper-vs-spacex-starlink (accessed: 31/12/2024).

Ramsey, B., An Ethical Decision-Making Tool for Offensive Cyberspace Operations, *Air & Space Power Journal*, 2018, 32(3).

Rogers, M.S., *Admiral, Address at the International Conference on Cyber Conflict*, NATO Cooperative Cyber Defense Centre of Excellence, Tallinn 2015.

Saboorian, A., A Brave New World: Using the Outer Space Treaty to Design International Data Protection Standards for Low-Earth Orbit Satellite Operators, *Journal of Air Law and Commerce*, 2019, 84(4), pp. 575–604.

Sanger, E., **Conger, K.**, Russia Was Behind Cyberattack in Run-Up to Ukraine War, Investigation Finds, *The New York Times*, 10 May 2022. Available at: https://www.nytimes.com/2022/05/10/us/politics/russia-cyberattack-ukraine-war.html (accessed: 31/12/2024).

Scholl, M., **Suloway, T.**, *Introduction to Cybersecurity for Commercial Satellite Operations*, National Institute of Standards and Technology, U.S. Department of Commerce, Washington 2023.

Sherlock, A., Blade Runner: 10 Tropes Of Film Noir (& How It Puts A Sci-Fi Twist On Them), *Screenrant*, 22 August 2020. Available at: https://screenrant.com/blade-runner-film-noir-tropes-sci-fi-twist/ (accessed: 31/12/2024).

Shipp, J.W., Space and Cyberspace: The Overlap and Intersection of Two Frontiers, *Army Space Journal*, 2011, 10(1), pp. 40–41.

Shweta, Aditham, K., **Hoeper, M.**, *What Is Threat Intelligence? Definition, Types & Process*, *Forbes Advisor*, 12 October 2023. Available at: https://www.forbes.com/advisor/business/what-is-threat-intelligence/ (accessed: 31/12/2024).

Smith, M., Anti-satellite weapons: History, types and purpose. *Space*, 10 August 2022. Available at: https://www.space.com/anti-satellite-weapons-asats (accessed: 31/12/2024).

Suwijak, Ch., Li, S., Global Internet Access from the Low Earth Orbit: Legal Issues regarding Cybersecurity in Outer Space, *Journal of East Asia and International Law*, 2022, 15(1).

Sznycer, A., **Patrick, C.**, Intuitions about justice are a consistent part of human nature across cultures and millennia, *The Conversation*, 21 October 2022. Available at: https://theconversation.com/intuitions-about-justice-are-a-consistent-part-of-human-nature-across-cultures-and-millennia-190523 (accessed: 31/12/2024).

Tracking and Tada Relay Satellite (TDRS): Continuing the Critical Lifeline, Goddard Space Flight Center, NASA. Available at: https://www.nasa.gov/wp-content/uploads/2022/04/tdrsfactsheet_3.pdf (accessed: 31/12/2024).

United Nations, *Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security*, UN Doc A/76/135, 14 July 2021, paragraph 18.

United Nations, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/68/98, 2013.

United Nations, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*, 27 January 1967, 610 UNTS 205, article II (entered into force 10 October 1967) [Outer Space Treaty].

Wheale, N., Recognizing a 'Human-Thing': Cyborgs, Robots and Replicants in Philip K. Dick's 'Do Androids Dream of Electric Sheep?' And Ridley Scott's 'Blade Runner', *Critical Survey*, 1991, 3(3), pp. 297–304.

Whitman, M., **Mattord, H.**, *Management of Information Security*, Cengage Learning, Boston 2016.

Williams, E., Ideology as Dystopia: An Interpretation of 'Blade Runner', *Revue Internationale de Science Politique*, 1988, 9(4).

Zurkus, K., What's the Value in Attack Attribution?, *CSO Online*, 2017. Available at: https://www.csoonline.com/article/560371/is-identifying-an-attacker-a-waste-of-time.html (accessed: 31/12/2024).

https://doi.org/10.18778/8331-719-9.07

Making Strides Towards Space Security in Low Earth Orbit

Laetitia Cesari[1]

Introduction

Once, space-based communication and broadcasting were mostly provided by geostationary satellites remaining fixed in position relative to a single region on Earth.[2] Today, the deployment of low Earth orbit (LEO) satellite constellations enables continuous coverage worldwide to adapt to broader and more dynamic demands for access to connectivity.[3] Additionally, space stations[4] and Earth observation satellites[5] are also important spacecraft placed in LEO. As space infrastructures are becoming increasingly important for the provision of essential services to populations and the support of military operations, so does the role of commercial space operators at all stages of a mission.[6]

---

1 University of Luxembourg, Luxembourg-Ville, Luxembourg.

2 Organisation for Economic Co-operation and Development, Satellite Communication: Structural Change and Competition, *OECD Digital Economy Papers*, 1995, 17, pp. 15–16.

3 C.D. Johnson, *The Legal Status of MegaLEO Constellations and Concerns About Appropriation of Large Swaths of Earth Orbit*, [in:] J. N. Pelton, S. Madry (eds.), *Handbook of Small Satellites*, Springer, Berlin 2020, pp. 1337–1339; C.L. Rachfal, Low Earth Orbit Satellites: Potential to Address the Broadband Digital Divide, *Congressional Research Service Report*, 2021, R46896, pp. 1–4.

4 A. Paravano, B. Rosseau, G. Locatelli, M. Weinzierl, P. Trucco, Toward the LEO economy: A value assessment of commercial space stations for space and non-space users, *Acta Astronautica*, 2025, 228, pp. 453–455.

5 Australian Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *Analysis of Low Earth Orbit Satellites*, Canberra 2024, p. 3.

6 V. Machi, US Military Places a Bet on LEO for Space Security, *Via Satellite*, June 2021. Available at: https://www.sda.mil/us-military-places-a-bet-on-leo-for-space-security/ (accessed: 03/02/2025); S. Wise, Eyes in the sky: The increasing importance of very low Earth orbit (VLEO) for national security, *SpaceNews*, 24 January 2024.

As space systems have evolved, so too has the context within which their missions are conducted. Generally, space-based assets supporting military and government activities are deployed with dedicated radio frequencies and customised configurations to operate separately from the general commercial network, ensuring secure and exclusive usage, with "wall off" solutions for governmental and military applications.[7] Yet, shared commercial networks can be used by military forces and public authorities, while benefitting civilian populations.[8] Technically, different user types can be routed through either distinct ground segments, acting like gateways, or virtualised network paths to specific customer groups. A unique network infrastructure can be segmented to allocate bandwidth and resources to separate civilian, commercial, military or governmental traffic.[9]

These dual use infrastructures have expanded the scope and impact of these collaborations: commercial entities now wield significant strategic power that was once the exclusive domain of State actors, placing them in a position that may influence both warfare and diplomacy.[10] At the same time, strategic operations supported by private commercial operators have posed many novel challenges in terms of space security.[11]

In the wake of geopolitical tensions, a debate is brewing about how to regulate and protect space assets, and particularly LEO satellite constellations. When employed by military forces or governments for strategic activities, should space assets deployed and operated by private operators receive the same level of scrutiny as other essential critical sectors? The question matters because when an asset qualifies as essential, regulation—and, subsequently, protection—is more likely to follow.

---

7 J. Jang-Jaccard, S. Nepal, A survey of emerging threats in cybersecurity, *Journal of Computer and System Sciences*, 2014, 80(5), p. 974, 979; J. Wolf, Special report: The Pentagon's new cyber warriors, *Reuters*, 5 October 2010.

8 N. Raju, Space security governance: steps to limit the human costs of military operations in outer space, *Humanitarian Law & Policy International Committee of the Red Cross*, 22 August 2023; S. Eves, G. Doucet, Reducing the civilian cost of military counterspace operations, *Humanitarian Law & Policy International Committee of the Red Cross*, 17 August, 2023.

9 F. Casaril, L. Galletta, Securing SatCom user segment: A study on cybersecurity challenges in view of IRIS2, *Computers & Security*, 2024, 140, p. 2; J. Suomalainen, J. Julku, M. Vehkapera, H. Posti, Securing Public Safety Communications on Commercial and Tactical 5G Networks, *IEEE Open Journal of the Communications Society*, 2 July 2021, p. 1595.

10 C.L White, Exploring the role of private-sector corporations in public diplomacy, *Public Relations Inquiry*, 2015, 4(3), pp. 305–321; M. Nagelmackers-Voïnov, *Business and Private Diplomacy*, no. 3, Geneva Centre for Security Policy, Geneva 2017, pp. 2–4, 12; C. Magee, How the UK and Nato are preparing for spectre of nuclear war in space, *The I Paper*, 12 January 2025. Available at: https://inews.co.uk/news/world/uk-nato-preparing-spectre-nuclear-war-space-3470073?srsltid=AfmBOorx2FA8KE0BDqN9FJn4qMNOWNpAAeB9fGlqkoBKibtoKcVSTNZ9 (accessed: 02/02/2025).

11 C. Poirier, The War in Ukraine from a Space Cybersecurity Perspective, *ESPI Short Report*, 2022, 1, p. 11. Available at: https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Short-1-Final-Report.pdf (accessed: 03/02/2025); T. Masson-Zwaan, M. Hofmann, *Introduction to Space Law*, Fourth Edition, Kluwer Law International, Alphen aan den Rijn 2019, pp. 72–73; L. Cesari, *Commercial Space Operators on the Digital Battlefield*, „A CIGI Essay Series: Cybersecurity and Outer Space", Centre for International Governance Innovation, 29 January 2023.

The following reflections attempt to move the debate on the security of LEO satellite constellations beyond the classic position that only States have a role to play in threat reduction processes. It raises two questions. Considering the first-order question, what are the main threats faced by space infrastructures, and particularly LEO satellite constellations? A second question follows accordingly: if private commercial entities provide strategic services, what then is the governance framework in place to regulate and protect them from threats?

This chapter proceeds in three sections. The first examines how LEO satellite constellations are a game changer for both space operators and users. The second section outlines the ways in which the increasing importance of dual use space systems impacts diplomatic discussions. The third and concluding section articulates some reflections for a potential path forward, from a governance perspective, including law and diplomacy, though it recognises there is no easy solution.

Global reach, instant access: the impact of LEO satellite constellations on modern communication systems

The evolution of technology in an increasingly interconnected world requires the continuous adaptation of infrastructure. As global digitisation advances, traditional models of industrial collaboration have given way to vertical integration to enhance innovation and reduce external dependencies.[12] This shift is paralleled by the deployment of low Earth orbit satellite constellations, reshaping the dynamics for both operators and users.

Technology evolution in an interconnected world: adapting infrastructures

Technology is the art of applying knowledge for practical purposes.[13] Increasingly essential to modern societies, information and communication technology (ICT) requires the use of devices, networks and digital capabilities to store, retrieve, process and transmit data for specific use cases.[14] Nowadays, the world's interconnection depends on ICT deployed, owned and operated across the globe by large consortia of communication and technology companies and governments.[15] Although licensed and monitored by States, infrastructure owners, Internet service

12 G. Denis, D. Alary, X. Pasco, N. Pisot, D. Texier, S. Toulza, From new space to big space: How commercial space dream is becoming a reality, *Acta Astronautica*, 2020, 166, pp. 436, 440–443.

13 *Technology*, Merriam-Webster's Collegiate Dictionary, 2025.

14 M.N.O. Sadiku, C.M.M. Kotteti, J.O. Sadiku, Information and Communication Technology: A Primer, *International Journal of Trend in Research and Development*, 2024, 11(3), pp. 171–174.

15 K. Jones, L. Gordon, Global Communications Infrastructure: Undersea and Beyond, *The Aerospace Corporation*, 3 February 2022, p. 7–8. Available at: https://csps.aerospace.org/papers/global-communications-infrastructure-undersea-and-beyond (accessed: 02/02/2025).

providers, manufacturers of digital devices and equipment, and editors of software, websites and applications are mostly private commercial entities.[16]

Big technology companies have not raised their profiles so dramatically only in recent years. Their role unwinds incrementally and is indispensable for essential and critical sectors (e.g. healthcare, finance, transportation, energy…)[17] and for military operations,[18] as ICT underpins operations, enables real-time communication and supports data and resources management. The important role ICT plays in these sectors, strategic activities, and democratic processes illustrates the tremendous potential stakes at play. Beginning with traditional infrastructure and networks, terrestrial and submarine cables historically form the backbone of modern communications, supported by space-based assets which serve as backhaul solutions for remote sites where laying cables is impractical. To put this into practice, traditionally, all stakeholders have to cooperate to foster interoperability between infrastructures and seamless integrations of the systems and applications.

After half a century punctuated by the placement of geostationary (GEO) satellites limited in speed, latency and capacity, space operators are shifting the market surprisingly quickly.[19]

This transformation occurred in different phases: initially, the geostationary orbit was the most coveted due to its unique characteristics, as placing an object in this orbit would guarantee its rotation is synchronous with the Earth's and, therefore, constantly cover the same region of the world, with only little adjustment needed.[20] Previously, communication networks were largely dedicated to single services, such as television, radio, or access to the Internet, with each operating independently through distinct links.[21] Ideal for applications that require consistent service over wide geographic areas, GEO satellites are also designed to operate with simpler and fixed ground infrastructure, with long life expectancy, reducing the number of satellites required and the need for frequent replacements or upgrades.[22]

---

16 *Ibidem*; M. Latzer, N. Just, F. Saurwein, P. Slominski, Institutional variety in communications regulation. Classification scheme and empirical evidence from Austria, *Telecommunications Policy*, 2006, 30(3–4), pp. 152–170; W.H. Read, Network control in global communications, *Telecommunications Policy*, 1977, 1(2), pp. 125–137.

17 Digital Security and Resilience in Critical Infrastructure and Essential Services, *OECD Digital Economy Papers*, 2019, 281, pp. 9–33.

18 H. Ullah, M. Uzair, Z. Jan, M. Ullah, Integrating industry 4.0 technologies in defense manufacturing: Challenges, solutions, and potential opportunities, *Array*, 2024, 23, pp. 1–2.

19 J. Foust, GEO satellite operators seek multi-orbit strategies, *Space News*, 26 January 2022. Available at: https://spacenews.com/geo-satellite-operators-seek-multi-orbit-strategies/ (accessed: 02/02/2025).

20 T. Sgobba, F.A. Allahdadi, *Orbital Operations Safety*, [in:] F.A. Allahdadi, I. Rongier, P.D. Wilde (eds.), *Safety Design for Space Operations*, Butterworth-Heinemann, Oxford 2013, pp. 411–415.

21 T. Pratt, J.E. Allnutt, *Satellite Communications, 3rd Edition*, Wiley-Blackwell, Hoboken, New Jersey 2019, pp. 543–633.

22 T.G. Roberts, C. Bullock, A sustainable geostationary space environment requires new norms of behavior, *MIT Science Policy Review. Communication*, 2020, 1, p. 34.

Then, the technical redesign of digital technology shuffled the deck in regard to a convergence of systems that integrate these multiple services into unified platforms. Now, homes, enterprises and public organisations are generally connected via a single terminal providing for diverse services, including multicast-based streaming on-demand systems such as video on-demand systems, applications, radio and direct access to the World Wide Web.[23]

Next come advances in space technology. LEO satellite constellations promise to challenge this paradigm, offering faster, lower latency, and more accessible global connectivity.[24] This technological evolution raises the possibility that satellite systems could one day significantly rival traditional infrastructure and networks in certain applications, marking a transformative evolution. Over-the-top services delivered directly to users have disrupted traditional business models and are increasingly interwoven with the infrastructure like LEO constellations, serving global audiences and transcending national boundaries.[25]

With the emergence of the Internet of Things and the multiplication of smartphones, several digital devices need access to connectivity to connect to the web and use applications.[26] This new paradigm led space operators and manufacturers to adapt to the multiplication of digital devices and equipment across the world and, consequently, develop multi-purpose software-defined satellite systems connected to a platform to provide for a wide range of integrated applications simultaneously.[27]

The production shift: from industrial collaboration to vertical integration

Taking stock of the many stakeholders generally involved in space activities is a way of understanding the complexity and multi-dimensional nature of the traditional space industry. Here, all of the stakeholders are involved and interconnected to different degrees. The issue can be examined from various perspectives, such as the entire supply chain or the phases of the mission, from the launching to the decommissioning of the space assets. Attempting to make a complete and exhaustive list becomes a perilous exercise, as each space mission is unique. Traditionally,

23 G. Fortino, C. Mastroianni, W. Russo, Computer Systems Cooperative control of multicast-based streaming on-demand systems, *Future Generation Computer Systems*, 2005, 21(5), pp. 823–839; J. Hess, B. Ley, C. Ogonowski, L. Wan, V. Wulf, Understanding and supporting cross-platform usage in the living room, *Entertainment Computing*, 2012, 3(2), pp. 37–47.

24 C.L. Rachfal, Low Earth Orbit Satellites: Potential to Address the Broadband Digital Divide, *Congressional Research Service Report*, 2021, R46896, pp. 6–12.

25 H. Jameson, OTT: New Business Models Disrupting the Satellite Industry, *Via Satellite*, 24 July 2023.

26 *Measuring the Internet of Things*, Organisation for Economic Co-operation and Development, 13 October 2023, pp. 12–14; T. Saarikko, U.H. Westergren, T. Blomquist, The Internet of Things: Are you ready for what's coming?, *Business Horizons*, 2017, 60(5), pp. 667–676.

27 *Software-defined satellite enters commercial service*, European Space Agency, Brussels 2022; W. Jiang, Software defined satellite networks: A survey, *Digital Communications and Networks*, 2023, 9(6), pp. 1243–1264.

space operators acting as service providers coordinate the stakeholders, including manufacturers customising space assets for specific missions and launch providers supplying the rockets, launch facilities and expertise needed to deploy the spacecraft.[28]

In the 2010s, some companies started to challenge the traditional cooperation model in the space industry, between launch service providers, manufacturers and operators.[29] Considering that reliance on outsourcing and external suppliers leads to inefficiencies and cost overruns, they transformed their business strategy to control as much of the production and operation process as possible, including timeliness and strategy. Unlike traditional operators that rely on subcontractors, these companies started a vertical integration process, developing, building and testing most of their rocket components, space assets and software in-house.[30]

LEO constellations are composed of a large number of satellites covering the Earth. Depending on the manufacturer, hundreds to several thousands of interconnected assets are necessary to constitute these systems. The design generally relies on production line methods, using the "on-the-shelf" technology and miniaturised subsystems.[31] To avoid extra weight, manufacturers abandon what is considered "secondary"—sometimes cybersecurity and protection measures.[32] Standard digital solutions are included in the payloads, with flexible and programmable components. These LEO satellites aim to provide high-speed connectivity and low latency for various purposes, including access to the Internet for example for "on the move" connectivity for aircraft, ships, vehicles, or trains.[33] LEO satellite constellations also mean a bigger number of links between space systems and the ground with a growing number of connected devices, with increased integration of satellite connectivity into various applications, such as data transfer and storage, cloud technologies, Internet of things, machine-to-machine, among other digital developments requiring high-speed real-time communication.

---

28 S. Rementeria, Power Dynamics in the Age of Space Commercialisation, *Space Policy*, 2022, p. 60.

29 A. Vernile, *The Rise of Private Actors in the Space Sector*, Springer, Berlin 2018.

30 C. Giannopapa, A. Staveris-Poykalas, S. Metallinos, Space as an enabler for sustainable digital transformation: The new space race and benefits for newcomers, *Acta Astronautica*, 2022, 198, pp. 728–732.

31 C. Henry, Modernizing Manufacturing: How to Build the Satellite of the Future, *Via Satellite*, 30 March 2016.

32 B. Bailey, Cybersecurity Protections for Spacecraft: A Threat Based Approach, *The Aerospace Corporation*, 29 April 2021; *Security architecture for space data systems*, The Consultative Committee for Space Data Systems, Washington D.C. 2012; D. Housen-Couriel, Cybersecurity threats to satellite communications: Towards a typology of state actor responses, *Acta Astronautica*, 2016, 128, p. 411; D.E. Cunningham, G. Palavicini Jr., J. Romero-Mariona, *Towards Effective Cybersecurity for Modular, Open Architecture Satellite Systems*, 30th Annual AIAA/USU Conference on Small Satellites, 21 July 2016, p. 1.

33 J. Rainbow, Dawn of the multi-orbit era, *SpaceNews*, 11 March 2024; A. Hsieh, V. Wu, Global maritime satellite market makes waves, *Digitimes Asia*, 11 December 2023; J. Reed, Leveraging LEO for Next-Generation In-Flight Connectivity, *Avionics International*, July/August 2023.

Henceforth, LEO satellite constellations are embedded in a global network and are subsequently becoming crucial for States. Because they constitute a system of systems composed of multiple assets, diverse utilisations and changing traffic paths, LEO constellations represent a shift in the architecture of space infrastructures and the way space connectivity works, moving from a standalone transponder onboard a stationary GEO satellite covering one point of the Earth's surface continuously to multiple interconnected assets rapidly rotating the globe and not fixed relative to a specific point on Earth. Due to their lower altitude, LEO satellites cover smaller areas and consequently need a large number of satellites to provide continuous coverage as each satellite passes quickly out of range.[34]

This new architecture also represents a change in terms of energy required and costs: GEO satellites are larger and more sophisticated assets necessitating long-range launchers capable of reaching large distances at almost 36,000 km altitude, while LEO satellite constellations, closer to the Earth, require less power and involve smaller and cheaper assets to manufacture and launch, though such systems involve more assets and require regular replenishment as individual satellites have shorter lifespans.[35]

Worldwide access to connectivity: the deployment of LEO satellite constellations as a turning point for operators and users

Describing the evolution of ICT—and the architecture of space missions—illustrates how use cases reshaped the market and, consequently, the type of infrastructures operated to support access to connectivity. For decades, the private sector, public authorities and important services necessary for human societies (electricity, transportation, water management, health, agriculture…) have been relying on space infrastructures to function properly.[36] These developments led technology companies and space operators to rethink services provided to customers. Several reasons explain the expansion of LEO satellite constellations, including a shift in the market and the evolution of population uses, with the significant place of digital services and smartphones in modern societies. Some activities, including information sharing, communication and command and control of connected objects, require high-speed connectivity and low latency, hence bolstering the deployment of global communication networks in outer space. Beyond the need for connectivity across the globe for fixed homes in populated areas, satellite operators started

34 L. Sodders, *LEO, MEO or GEO? Diversifying orbits is not a one-size-fits-all mission (Part 1 of 3)*, US Space Operations Command, 18 July 2023.

35 J.B. Clark, *The Space Environment: An Overview*, [in:] L.R. Young, J.P. Sutton (eds.), *Handbook of Bioastronautics*, Springer, Cham 2021, pp. 23–57.

36 M. Pellegrino, G. Stang, *Space security for Europe*, European Union Institute for Security Studies, Brussels 2016, pp. 21–36.

to consider remote locations to bridge the digital gap and provide access to connectivity all around the world.[37]

This description also shows the shift from the limited provision of localised services to the broad deployment of networks constantly covering the surface of the planet. The deployment and regulation of connectivity infrastructures are a significant undertaking. The traditional infrastructures forming the backbone of communications are constituted by complementary networks and equipment whose deployment and operation are regulated by public authorities.[38] Such regulations include the right to use public and private land within a country to deploy terrestrial networks, to obtain licenses for radio spectrum allocation concerning wireless networks (e.g. mobile and satellites),[39] or to lay submarine cables on the bed of the high seas beyond the continental shelf.[40] Interconnection between different these infrastructures requires technical coordination to ensure seamless data transmission, regulatory compatibility, and legal cooperation so States can make sure data passing through their countries is not intercepted or used unlawfully. Regulatory compatibility plays a significant role in coordination between interconnected States, because of differences in technical standards, data privacy laws, tariffs and customs.[41] However, at the border of interconnected States, challenges can arise when managing data and information and communication networks, and lead to bottleneck or restricted data flows.[42] In some cases, States may decide to route all international data flows through a small number of controlled infrastructures and isolate domestic traffic from the global network.[43]

A satellite operator providing broadband Internet and television broadcasting in a country must comply with that country's laws, including the granting of business

37 R. McMahon, M. Akcayir, B. Norris, L. Fabian, *Assessing the Impacts of Low-Earth Orbital Satellite Systems in Remote Indigenous Communities: Social and Economic Outcomes of Use in Northern Canada*, *Satellites and Beyond*, SSRN, 2024. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5012799 (accessed: 02/02/2025).

38 A. González Fanfalone, M. Reisch, M. Naito, J. Lee, V. Weber, Bridging connectivity divides, *OECD Going Digital Toolkit Notes*, 2021, 16, pp. 12–18.

39 International Telecommunication Union and the World Bank, *Overview of national spectrum licensing*, 6 October 2020; International Telecommunication Union, *ITU-R: Managing the radio-frequency spectrum for the world*, August 2024.

40 United Nations, *Convention on the Law of the Sea*, Articles 87 and 112; E. Wagner, Submarine cables and protections provided by the law of the sea, *Marine Policy*, 1995, 19(2), pp. 127–136.

41 International Regulatory Co-operation, *OECD Best Practice Principles for Regulatory Policy*, Organisation for Economic Co-operation and Development, Paris 2021, p. 22, 59.

42 J. Steinbart, Problems and Issues in the Management of International Data Communications Networks: The Experiences of American Companies, *MIS Quarterly*, 1992, 16(1), pp. 55–76; V. Bekkers, M. Thaens, Interconnected networks and the governance of risk and trust, *Information Polity*, 2005, 10(1–2), pp. 37–48; N. Cory, L. Dascoli, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, Information Technology & Innovation Foundation, Washington D.C. 2021.

43 L. Salamatian, F. Douzet, K. Salamatian, K. Limonier, The geopolitics behind the routes data travel, *Journal of Cybersecurity*, 2021, 7(1).

licenses and landing rights.[44] Without it, an operator cannot connect its infrastructures to domestic networks or beam signals within a national territory. Yet, the control that States exercise through permissions granted to operators is being challenged.[45] Not only do LEO satellite constellations provide continuous global coverage without the need for fixed ground stations in every country, but they can also directly connect to user terminals with satellite dishes and may soon enable direct-to-cell services.[46] Direct transmission is now possible worldwide without physical presence or clear point of entry, which reduces the operators' dependency on permissions and subsequently hinders States willing to manage or block data transmitted by LEO satellite constellations and monitor the content of communications.[47]

States can consider that LEO satellite constellations challenge their ability to regulate, monitor and control external connectivity within their national borders.[48] This raises significant concerns regarding space security and makes diplomatic discussions more complex.

The reason why this section describes this situation is twofold. States may view foreign-controlled LEO satellite constellations as a risk to their sovereignty and control over national ICT and infrastructures.[49] Furthermore, non-authorised users may also acquire equipment to connect to these networks without permission through unofficial channels.[50] Rogue actors, non-State entities, or even military

---

44 J.N. Pelton, Defining a communications satellite policy system for the 21st century: A model for an international legal framework and a new "code of conduct", *Acta Astronautica*, 1996, 38(4–8), pp. 577–585; J. Kulesza, B. Akcali Gur, Satellite Internet Access in Times of Cyber Conflict, *Directions*, 28 April 2022; J. Foust, SpaceX worked for weeks to begin Starlink service in Ukraine, *SpaceNews*, 8 March 2022; M. Evans, Overcoming Landing Rights Issues to Expand Access to Satellite, *Via Satellite*, 23 August 2024.

45 Regulation of NGSO Satellite Constellations, International Telecommunication Union and the World Bank, *Digital Regulation Platform*, 28 March 2024; A.C. Boley, M. Byers, Satellite mega-constellations create risks in Low Earth Orbit, the atmosphere and on Earth, Scientific Reports, 2021, 11(10642).

46 J. Rainbow, SpaceX gets conditional approval for direct-to-smartphone service, *SpaceNews*, 26 November 2024; Federal Communications Commission, *Order and Authorization DA 24-1193*, 26 November 2024.

47 R. Feasey, A. de Streel, P. Alexiadis, M. Bourreau, M. Cave, I. Godlovitch, A. Manganelli, G. Monti, T. Shortall, P. Timmers, *The Future of European Telecommunications: In-depth Analysis*, Centre on Regulation in Europe, Brussels 2024, pp. 17–28.

48 *Ibid*em; A.P. Zucherman, B.M. Braun, E.M. Sims, Space Safety Laws & Regulations: Navigating the policy compliance roadmap for small satellites, *Journal of Space Safety Engineering*, 2022, 9(4), pp. 582–599; M.C. Mineiro, An inconvenient regulatory truth: Divergence in US and EU satellite export control policies on China, *Space Policy*, 2011, 27(4), pp. 213–215; K. Singh, D. Psaledakis, U.S. Treasury says some satellite internet equipment can be exported to Iran, *Reuters*, 20 September 2022.

49 B. Akcali Gur, J. Kulesza Equitable access to satellite broadband services: Challenges and opportunities for developing countries, *Telecommunications Policy*, 2024, 48(5), pp. 1–9.

50 Tech State, Starlink Cracks Down on Unauthorized Roaming, Disconnects Users in Africa, *Tech Estate*, 16 April 2024; AFP, Smuggled Starlink dishes throw lifeline to some in war-torn Sudan, *France24*, 3 April 2024.

forces can bypass government approval and operators consent to divert access to the Internet.[51] In some other situations, civilians located in regions with limited Internet access may be tempted to smuggle in user terminals to connect to LEO satellite constellations, circumventing State control. In some cases, even unauthorised, access to LEO networks can have positive effects, such as providing populations with uncensored communication or enabling connectivity in disaster zones.[52]

Other concerns are expressed towards LEO satellite constellations regarding States' sovereignty and control over their information and communication networks. As they are deployed between 300 and 400 km altitude, below most of the other space-based assets, some States fear that LEO satellite constellations can intercept data transmission between strategic satellites and their ground stations or interfere with radio signals.[53] These concerns are further compounded by criticisms, ranging from light pollution issues to space debris and the sheer logistical complexity of launching and maintaining such a network, especially at a low altitude.

Mitigation measures can be implemented by space operators to tackle these issues. For example, "geo-fencing" access and control over unauthorised regions; anomaly detection measures to identify unusual activity or user patters; monitoring distribution of terminals to limit their availability to authorised areas and users; user authentication to prevent the activation and utilisation of a terminal by external or unauthorised users, etc.

The central role of States in the utilisation and exploration of outer space

The characterisation of outer space as a Far West, unregulated and lawless, is both inaccurate and misleading. Contrary to this perception, space activities are governed by a comprehensive framework of international legal instruments, most notably the Outer Space Treaty of 1967,[54] which numerous States have been ratified. These agreements establish clear legal principles, including the peaceful use of outer space, liability for damages, and the international responsibility of States for activities conducted by both governmental and non-governmental entities. While challenges persist in ensuring compliance and enforcement, it remains incumbent upon all relevant stakeholders, whether States, private actors, or international organisations, to fulfil their legal obligations and contribute to the sustainable and responsible use of outer space.

---

51 C. Steer, *International Humanitarian Law in the "Grey Zone" of Space and Cyber*, „A CIGI Essay Series Cybersecurity and Outer Space", Centre for International Governance Innovation, Waterloo, Ontario 2023.

52 A. Tobias, W. Leibrandt, J. Fuchs, A. Egurrola, Small satellites: Enabling operational disaster management systems, *Acta Astronautica*, 2000, 46(2–6), pp. 101–109.

53 J. Pelton, *Radio-Frequency Geo-location and Small Satellite Constellations*, [in:] J.N. Pelton (ed.), *Handbook of Small Satellite*, Springer Reference, Cham 2020, pp. 1–13.

54 United Nations, 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}, UNTS Vol. 610, No. 8843.

States' international responsibility for national activities and liability for damages

In practice, the conduct of space missions falls under specific rules of international space law.[55] One of these rules concerns States' responsibility for national space activities. Article VI of the Outer Space Treaty requires a State to authorise and supervise space activities.[56] States are internationally responsible for national activities and, in the event of a wrongful act, will be held accountable in accordance with their obligations. Often, a State will adopt a national legal framework with a licence process that implies imposing obligations on operators and minimum protection requirements on space objects.[57] These conditions should align with international obligations, particularly under the UN space-related treaties, and ensure that space activities are conducted safely, minimising risks to people, the environment, and property.

States generally appoint public authorities to supervise space companies and oversee the authorisation process, ensuring that relevant space activities comply with national security interests and international norms.[58] These authorities can range from governments, ministries of the government, special governmental committees, or national space agencies. Some activities, such as the coordination of the frequency spectrum, may require distinct licenses from different governmental entities recognised by the International Telecommunication Union.[59] However, States sometimes apply different conditions and processes to governmental, academic and military entities as well as to the private sector.[60]

Regarding the registration of space objects, as required by Article VIII of the Outer Space Treaty, an appropriate authority generally maintains a national registry of launched objects.[61] States can request notification when a space object becomes non-functional so this information can be submitted to the Secretary-General of the United Nations in accordance with the Registration Convention.

Parallel to these responsibility-related aspects, Article VII of the Outer Space Treaty concerns liability for damage,[62] either accidental or not. To address potential

55 T. Masson-Zwaan, M. Hofmann, *Introduction to Space Law*, Kluwer Law International, Alphen aan den Rijn 2019, pp. 45–47.

56 Outer Space Treaty, Article VI; T. Masson-Zwaan, M. Hofmann, *Introduction to Space Law*, Kluwer Law International, Alphen aan den Rijn 2019, p. 20.

57 M.A. Viscio, N. Viola, R. Fusaro, V. Basso, Methodology for requirements definition of complex space missions and systems, *Acta Astronautica*, 2015, 114, pp. 80–81.

58 T. Masson-Zwaan, M. Hofmann, *Introduction to Space Law*, Kluwer Law International, Alphen aan den Rijn 2019, pp. 47–50.

59 United Nations, *Constitution of the International Telecommunication Union, adopted at the Additional Plenipotentiary Conference, as amended by subsequent plenipotentiary conferences*, UNTS vol. 1002; International Telecommunication Union, *Guidelines for the Preparation of a National Table of Frequency Allocations (NTFA)*, Telecommunication Development Sector 2015, p. 8.

60 UNOOSA, *Registration of Objects Launched Into Outer Space, Stakeholder Study*, Vienna 2023, p. 7.

61 Outer Space Treaty, Article VIII

62 Outer Space Treaty, Article VII.

liability for damage caused by space objects, domestic legislations tend to define how operators or owners of space objects seek recourse. This often involves an insurance contract indemnifying the launching State for compensation costs. Requiring appropriate insurance coverage from space object owners or operators is thus a key method for launching States to manage risk when authorising entities under their jurisdiction.[63]

However, within all national laws framing the authorisation of space activities, there is no common reference framework containing shared definitions and rules for space activities, assets, components, protection methods, and digital content. States have a wide room for manoeuvre with regard to what the legal framework applicable at the international level to space activities prescribes.[64]

State various approaches to space missions authorisation and supervision

Global reliance on space infrastructure raises several questions regarding influence, control and sovereignty. These past few years, the importance of private operators increased, and their influence over national regulations grew drastically. Although States keep an important role in authorising and supervising space activities, views on the necessity to implement strict rules and criteria for mission authorisation, control and supervision of corporate activity, can differ from one government to another.

Some States retain strong jurisdiction over their space industry with strict authorisation and supervision mechanisms.

The conditions for issuing authorisations may, for example, be subject to stringent requirements, particularly with regard to the launch, control and transfer of control of a launched space object and its re-entry to Earth. In this context, public authorities can verify the moral, financial and professional guarantees of the applicant and, where applicable, its shareholders. Public authorities may also check the conformity of the systems and procedures with technical regulations and standards. The competent administrative authority may also regulate space-enabled applications. To this end, it ensures that space operators' activities do not undermine a State's interests, in particular national defence, foreign policy and the State's international commitments. It may, at any time, prescribe any restrictions on operators' activities necessary to safeguard these interests. Moreover, public authorities may also ask space operators to interrupt the provision of space services to foreign States for strategic or political reasons.[65]

Another example of strong supervision mechanisms is the requisition regime. States can adopt domestic laws enabling public authorities or military forces to seize control of space assets and of the execution of services for national interests when the

63 I.I. Kuskuvelis, The space risk and commercial space insurance, *Space Policy*, 1993, 9(2), pp. 109–120.

64 Outer Space Treaty, Article VI; Registration Convention, Article V.

65 J. Davalos, International Standards in Regulating Space Travel: Clarifying Ambiguities in the Commercial Era of Outer Space, *Emory International Law Review*, 2016, 30(4), pp. 610–611.

required goods or services are unavailable or inaccessible in another manner.[66] This mechanism allows public authorities to address material deficiencies by resorting to temporary actions. Such measures are, however, generally combined with compensatory arrangements to mitigate the burden placed on the requisitioned parties.

Conversely, other States can choose a more permissive approach regarding mission authorisation, control and supervision of corporate activity. Considering that regulatory flexibility encourages private sector growth and attract investment, some States may implement regulatory frameworks that are less stringent compared to the ones mentioned above. For instance, public authorities can implement expedited licensing procedures and lower compliance costs.[67] By adopting a permissive stance, States can focus on meeting only the minimum requirements of international law and choose not to consider some provisions provided in international guidelines such as the Space Debris Mitigation Guidelines[68] and the Long-Term Sustainability Guidelines.[69] Moreover, States may entrust private corporations with greater self-regulation and oversight responsibilities, allowing industry-led standards and best practices to guide safety, environmental, and operational procedures, reducing the direct involvement of governmental bodies. Although such a permissive approach might lead to regulatory arbitrage, where companies choose to operate under the jurisdiction with the least restrictive requirements, potentially undermining global efforts for responsible space governance, some States consider it to constitute innovation incentives and economic opportunities for their national space industry.

The rise of private companies in global geopolitics: a shifting balance of power

Historically, States have maintained strict control over their domestic companies, with comprehensive oversight to ensure compliance with national laws and policies. However, in recent years, private industry has assumed a prominent role in areas traditionally dominated by States, including military operations and support to strategic activities such as satellite communications and intelligence gathering.[70] LEO satellite constellations deployed and operated by the private sector are

66 i.e. France, Ordonnance n° 2022-232 du 23 février 2022 relative à la protection des intérêts de la défense nationale dans la conduite des opérations spatiales et l'exploitation des données d'origine spatiale, *Journal officiel de la République française*, 2022, No. 0046; P. Clerc, Les enjeux juridiques de l'observation de la Terre depuis l'espace dans le contexte de la nouvelle économie spatiale, *Enjeux numériques*, 2024, p. 49.

67 J. Roulette, Exclusive: Trump likely to axe space council after SpaceX lobbying, sources say, *Reuters*, 21 January 2025.

68 United Nations Office for Outer Space Affairs, *Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space*, 2007, UN Doc. A/62/20, Annex.

69 United Nations Office for Outer Space Affairs, *Guidelines for the Long-term Sustainability of Outer Space Activities of the Committee on the Peaceful Uses of Outer Space*, 2019, UN Doc. A/AC.105/118.

70 S. Erwin, Private satellite operators make case for helping military track ground targets, *SpaceNews*, 23 March 2024.

increasingly used for governmental and military purposes. These space-enabled applications are not only being offered to their national States but are also being extended to foreign States, creating complex dynamics in international relations and national security considerations.[71] This situation presents several concerns regarding their use by different State powers. When a LEO satellite constellation is owned and operated by multinational corporations, it may create dependency on companies which may not align with a foreign States user's national interests or policies. Moreover, the dual nature of space assets can make the entire network a target during geopolitical tensions, even if it serves civilian purposes too.[72]

State users are not guaranteed continuous service for specific operations or in regions with limited commercial value. It also means that these users may lose access to these services during crises if the private company refuses the provision of services or delays service adjustments that conflict with their commercial interests, increasing disparities between customers. Because private companies prioritise profitability and are subject to market forces, including political and economic shifts. The same goes in times of high demand (during a disaster and in times of tensions): private operators may prioritise commercial customers over governments, users, unless pre-agreed contracts ensure priority access. Finally, as the initial purpose of commercial operators is to be cost-efficient and prioritise benefits, they may not prioritise investments in stringent security protocols required for sensitive government and military communications. This dependency can also lead to higher costs or unfavourable terms for foreign governments. Legal conflicts of laws and jurisdictions can also play a role in a company's reluctance or lack of compliance with government demands.

Finally, another concern lies in the lack of operational transparency. Even though users, whether governmental or non-governmental, benefit from the network, they are not informed about internal organisation and management, including potential vulnerabilities and disruptions,[73] because of the sensitive nature of such disruption, but also companies' need to protect their reputation, as successful intrusions or disruptions tend to be kept secret. Operators and even States tend to limit the sharing of details to prevent other threat agents from taking advantage of vulnerabilities and adding pressure on national infrastructures. This complexity constitutes a potential challenge for users of LEO satellite constellations, if they become too dependent on such infrastructure.

Because of these considerations, LEO constellations need to be examined through the space security lens with a particular focus on the threat landscape and potential risks faced by such infrastructures.

---

71 A. Melamed, A. Rao, O. de Rohan Willner, S. Kreps, Going to outer space with new space: The rise and consequences of evolving public-private partnerships, *Space Policy*, 2024, 68, p. 1.

72 J. West, J. Miller, Clearing the Fog: The Grey Zones of Space Governance, *CIGI Papers*, 2023, 287, p. 16.

73 J. Robinson, Transparency and confidence-building measures for space security, *Space Policy*, 2016, 37, pp. 134–144.

Mitigating controversies in outer space: the thin line between disagreement and conflict

In times of international tensions, States tend to adopt strategic postures, determining how their government and non-government entities will respond to certain events. These postures can guide the type of engagement they directly conduct against competitors and adversaries and the support they will provide to their allies and other third parties.

Threats faced by LEO constellations

Space infrastructures are typically constituted of a space segment and a ground segment. The former encompasses space-based assets, which include any spacecraft, and their component parts, launched into orbit. The latter consists of terrestrial infrastructure, including ground stations, required to operate space objects and deliver services, such as satellite dishes, satellite operation centres and receiving stations. Data links facilitate communication between the space and ground segments, with uplinks and downlinks. While exchanging on practical measures for the prevention of an arms race in outer space, experts recognised that the main threats to or involving space systems tend to emanate from four vectors: earth-to-space, space-to-earth, space-to-space and earth-to-earth.[74]

Space threats are disruptions and interferences by space objects and activities caused by the use of counterspace capabilities/space weapons,[75] which can be defined as "capabilities, techniques, or assets that can be used against another space object or a component of a space system in order to deliberately deny, disrupt, degrade, damage or destroy it reversibly or irreversibly, so as to gain an advantage over an adversary".[76]

LEO constellations are more vulnerable to a range of threats due to their relatively low altitude and the use of smaller, less sophisticated systems compared to traditional satellites. Besides internal malfunctions causing failures within the space infrastructure or accidental collisions in outer space, especially because it can be a lot more difficult to predict trajectory in LEO due to drag, a perturbing force that alters an asset's path,[77] LEO constellations can be subject to intentional

74 United Nations, Group of Governmental Experts on Further Practical Measures for the Prevention of an Arms Race in Outer Space, *Report of the Group of Governmental Experts on further practical measures for the prevention of an arms race in outer space*, 2024, UN Doc. GE-PAROS/2024/CRP.4.

75 A. Azcárate Ortega, V. Samson, Counterspace Capabilities: Renewed Hope for Cooperative Governance?, CIGI Papers, 2025, 313, p. 1.

76 A. Azcárate Ortega, V. Samson (eds.), *A Lexicon for Outer Space Security*, United Nations Institute for Disarmament Research, Geneva 2023, p. 38.

77 A.D. Hayes, R.J. Caverly, Model predictive tracking of spacecraft deorbit trajectories using drag modulation, *Acta Astronautica*, 2023, 202, pp. 670–685.

incidents potentially leading to service disruptions and data breaches. For example, damages can be caused by a direct hit to a space-based asset (i.e. direct-ascent or co-orbital anti-satellite (ASAT) technologies) or physical sabotage against the ground segment. Similarly, threat agents can conduct malicious cyber activities and exploit breaches within the space infrastructure to access a system or disrupt it. Moreover, data links can face signal interference and interception. The low altitude of LEO constellations makes them more susceptible to jamming and spoofing attacks, as signal transmissions have shorter travel distances from the ground and can be more easily intercepted or disrupted by relatively low-cost ground equipment.

Generally, satellites constituting LEO constellations embed fewer components and protection mechanisms, which can lead to reduced security measures in both hardware and software. This makes them more susceptible to cyber intrusions, where threat agents can exploit vulnerabilities to hijack control, intercept sensitive data, or degrade services. The increased number of satellites in LEO constellations also expands the potential attack surface, as a single compromised satellite can have cascading effects on the broader network. Moreover, the need for frequent replenishment and satellite replacement creates additional risks during the launch and deployment phases, offering further opportunities for interference.

The increasingly important world's reliance on space-based applications in State defence and security, governmental services, economy, public and critical infrastructures and global communication puts them at risk: space assets are becoming critical. A high-critical infrastructure is, by definition, a prime target for these types of threats, so it is crucial to identify and plug the likelihood, scale and effects of such disruptive activities. This means operators have to put in place advanced monitoring systems, intrusion detection mechanisms and rapid response capabilities to counter any harmful consequences of these space threats to the space mission.

Even if a space threat is successfully used against a satellite within a LEO constellation, the inherent design of these constellations, comprising a large number of relatively small assets, provides a degree of resilience and redundancy. Unlike satellites placed in geostationary orbit, LEO constellations are built to function as distributed networks. Consequently, the loss of a single or even multiple satellites does not necessarily result in a complete mission failure. Distributed redundancy allows operators to reroute functions across remaining operational satellites, maintaining overall system performance with minimal disruption. Moreover, some operators are working on responsive systems to ensure substitution in case of "lack, failure or degradation of existing space assets"[78] and quickly launch backup assets to replace the initial one. Yet, concerns exist regarding the potential for cascading effects following a strike that generates a large number of space debris. This poses long-term risks to the entire orbit and complicates future operations, as debris can indiscriminately collide with any object on its trajectory.

78 REACTS, Responsive Space Cluster Competence Center, DLR.

Examining the consequences of risks and threats caused in LEO reveals the ways disruptions can affect the use of some orbital shells, and the role State and private entities play in this context, from a legal and policy perspective.

The role of the 1967 Outer Space Treaty regarding space security

The Outer Space Treaty of 1967 contains important principles governing States' space activities, including the common interest of all humankind in the peaceful exploration and use of outer space[79] and freedoms of use and exploration by all States.[80] However, it also establishes an important limitation to these freedoms, namely, the prohibition of placing nuclear weapons or any other weapons of mass destruction in outer space, including in orbit around Earth, on celestial bodies, or in any other manner.[81]

This limitation, contained in Article IV, does not impose a "blanket prohibition" on military activities in outer space as long as they do not involve weapons of mass destruction or aggressive actions.[82] Consequently, States have conducted activities such as reconnaissance, surveillance, missile warning systems, and secure communications to support military operations on the ground. Some States interpreted this Article extensively and tested ASAT technologies against their own space-based assets, especially in LEO, including direct-ascent missiles[83] and cyber disruptions.[84] Furthermore, because the Outer Space Treaty does not explicitly address conventional weapons or the misuse of radio signals for offensive purposes in outer space, disruptive activities involving spacecraft have been reported by States, including close approaches by inspector satellites and jamming and spoofing against satellite communications.

With the emergence of new activities and new technologies, the question arises as to whether the existing legal framework applicable to space activities should be interpreted broadly to cover more disruptive practices or whether it should be supplemented with new measures that are more relevant and closer to reality.

79 Outer Space Treaty, Preamble.

80 Outer Space Treaty, Article I.

81 Outer Space Treaty, Article IV.

82 F.G. von der Dunk, Armed Conflicts in Outer Space: Which Law Applies?, *International Law Studies*, 2021, 188(97), p. 202; J. Grunert, The "Peaceful Use" of Outer Space?, *War on the Rocks*, 22 June 2021.

83 A. Azcárate Ortega, L. Cesari, *The road to a moratorium on kinetic ASAT testing is paved with good intentions, but is it feasible?*, Fondation pour la Recherche Stratégique, Paris 2022; The White House, *Remarks by Vice President Harris on the Ongoing Work to Establish Norms in Space*, 18 April 2022; N. Raju, *Russia's anti-satellite test should lead to a multilateral ban*, Stockholm International Peace Research Institute, Stockholm 2021; M. Aho, *United States Remarks for Conference on Disarmament Subsidiary Body 3 – Prevention of An Arms Race in Outer Space*, Washington D.C., March 22, 2022.

84 Thales, Thales Seizes Control of ESA Demonstration Satellite in First Cybersecurity Exercise of its kind, *Thales Group*, 25 April 2023.

The development of the law of outer space has been made possible by a number of factors driven by the States.[85]

States have deliberately developed and considered customary international law, taking into account good practice and the needs present. By acting in a certain way in the context of their space activities, whether as operators, authorising States, or recipients of space services, States can adopt an attitude that approves or condemns them. When certain States breach international law, the silence of other States may be perceived as a form of implicit concession, also qualified as "acquiescence[86]," which may weaken the norm violated and contribute to its alteration into customary international law. On the other hand, publicly condemning such violations reaffirms the norm in question and prevents it from being eroded. The "erosion of frameworks" has been, according to the UN Secretary-General, one of the factors of the current challenges faced by States when trying to negotiate on disarmament-related topics.[87] Therefore, this explicit condemnation is essential to maintain the strength and stability of international rules by sending a clear signal that the international community does not accept contrary behaviour instead of precluding the wrongfulness of the act.[88] However, a decision adopted at the international level is not necessarily that of the majority of States but rather that of a plurality of States that can influence these rules. It should be noted that in the process of adopting treaties, diplomacy is important. States form alliances and align themselves behind other States, whether they are small, intermediate or big powers, that carry or sponsor a text to collectively tackle an issue. With regards to space activities, this situation is quite frequent to push for specific principles or initiatives.[89]

Diplomatic discussions to prevent an arms raise in outer space

Considering that space security concerns could lead to an arms race and escalation of tensions between States, diplomacy has been used to strengthen international legal frameworks and promote stability, transparency and confidence-building.[90]

---

85 B. Cheng, *Studies in International Law*, Clarendon Press, Oxford 1997, p. 679.

86 E. Henry, Alleged Acquiescence Of The International Community To Revisionist Claims Of International Customary Law (With Special Reference To The Jus Contra Bellum Regime), *Melbourne Journal of International Law*, 2018, 18, pp. 10–11.

87 United Nations Secretary-General, *Secretary-General Urges Conference on Disarmament to Move Humanity Closer to Peace*, UN Doc. SG/SM/22139, 26 February 2024.

88 International Law Commission, Articles on the Responsibility of States for Internationally Wrongful Acts, UN Doc. A/RES/56/83, Article 45.

89 United Nations, *Recommendations on Possible Norms, Rules and Principles of Responsible Behaviors Relating to Threats by States to Space Systems, submitted by the Federal Republic of Germany and the Republic of the Philippines, Open-ended Working Group on Reducing Space Threats through Norms, Rules and Principles of Responsible Behaviours*, 2023, UN Doc. A/AC.294/2023/WP.1.

90 X. Pasco, *Enhancing Space Security in the Post Cold War Era: What Contribution from Europe?*, [in:] J.M. Logsdon, A.M. Schaffer, *Perspectives on Space Security*, Space Policy Institute, George Washington University, Washington D.C. 2005, pp. 51–68.

Since the 1980s, States delegations to the Conference on disarmament debate space-security related topics under the "Prevention of an arms race in outer space" (PAROS) agenda item. Working on the promotion of both "hard law" and "soft law" to tackle threats faced by space activities and tightening the net around disruptive operations conducted by threat agents, States are involved in various initiatives.[91] These efforts range from the negotiation of a legally-binding instrument to the development of non-binding measures and, sometimes, lead States to make unilateral pledges. During the debates, experts also proposed some transparency and confidence-building measures to reduce tensions.

More recently, main points of discussion have emerged that States should agree on what qualifies as responsible or irresponsible behaviours in outer space and adopt voluntary measures. These discussions focusing on the potentially disruptive consequences of a space mission are complemented by debates on further practical measures for the prevention of an arms race in outer space, including the characterisation of weapons placed in outer space and definitions and verification of threats emanating from any vector, also called "counterspace capabilities."

As an example, the use of direct-ascent counter-space capabilities in 2021 prompted rapid responses due to their disruptive effects, among which the creation of debris.[92] In reaction, Several States adopted unilateral acts and pledged never to launch such counter-space capabilities, which contributed to the drafting of an international resolution.[93] This momentum shows a growing willingness to regulate counter-space capabilities to avoid an escalation of tensions and preserve security in space. This situation is quite exceptional as negotiations at the multilateral process take time, especially when disarmament-related and discussions on PAROS have been slow for a long time at the Conference on Disarmament.[94] It is, therefore, a question of striking a balance between general negotiations aimed at framing a situation and allowing coordination between the different practices undertaken throughout the world and the action necessary to obtain mutual

91 United Nations Institute for Disarmament Research, *A Brief Overview of Norms Development in Outer Space*, Geneva 2012, p. 7.

92 A. Azcárate Ortega, L. Cesari, *The road to a moratorium on kinetic ASAT testing is paved with good intentions, but is it feasible?*, Fondation pour la Recherche Stratégique, Paris 2022; The White House, *Remarks by Vice President Harris on the Ongoing Work to Establish Norms in Space*, April 18, 2022; N. Raju, *Russia's anti-satellite test should lead to a multilateral ban*, Stockholm International Peace Research Institute, Stockholm 2021; U.S. Mission Geneva, M. Aho, *United States Remarks for Conference on Disarmament Subsidiary Body 3 – Prevention of An Arms Race in Outer Space*, March 22, 2022. Available at: https://geneva.usmission.gov/2022/03/22/cd-prevention-of-an-arms-race-in-space/ (accessed: 02/02/2025).

93 United Nations General Assembly, *Resolution adopted by the General Assembly on 7 December 2022 [on the report of the First Committee (A/77/383, para. 16)] 77/41, Destructive direct-ascent anti-satellite missile testing,* 2022, UN Doc. A/RES/77/41.

94 R.T. Grey, Jr., Deadlocked and Waiting at the UN Conference on Disarmament, interview by Wade Boese, *Arms Control Today*, Dec. 2000; *United Nations Secretary-General, Secretary-General Urges Conference on Disarmament to Move Humanity Closer to Peace*, 2024, UN Doc. SG/SM/22139.

understanding and reciprocal trust between States, at a given moment or over a more extended period.

Parallel to discussions on voluntary measures, States have proposed the development of legally binding measures, such as the Treaty on the Prevention of the Placement of Weapons in Outer Space,[95] the Threat or Use of Force Against Outer Space Objects (PPWT), presented to the Conference on Disarmament in 2002, 2008[96] and then revised in 2014,[97] incorporating feedback and addressing some concerns raised regarding verification and definitions of prohibited activities in the first version of the draft. Proposing a definition of weapon, sponsors to the draft PPWT suggested that the "term «weapon in outer space» means any device placed in outer space, based on any physical principle, which has been specially produced or converted to destroy, damage or disrupt the normal functioning of objects in outer space, on the Earth or in the Earth's atmosphere, or to eliminate a population or components of the biosphere which are important to human existence or inflict damage on them.[98]" The proposed definition, although contested, provides a basis for analysing the different types of threats in outer space and their potential impact on international security.

Recently, efforts within the Group of Governmental Experts (GGE) on Further Practical Measures for the Prevention of an Arms Race in Outer Space have aimed to establish clear legal norms to prevent the weaponisation of outer space, promote best practices to enhance space security and reduce the risk of conflict.[99]

Conclusion

Space security is particularly essential to LEO due to the critical role of space-based assets, particularly constellations, in supporting essential services, economic activities, and national security. Moreover, LEO is becoming increasingly

95 United Nations, *Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects (PPWT),* 2002, UN Doc. CD/1579.

96 United Nations, *Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects (PPWT)*, 2008, UN Doc. CD/1831; J. Su, The "peaceful purposes" principle in outer space and the Russia–China PPWT Proposal, *Space Policy* 2010, vol. 26, issue 2, pp. 81–90.

97 B. Britt, The PPWT and Ongoing Challenges to Arms Control in Space, *Joint Force Quarterly*, 2024, 113, pp. 81–85; F. Tronchetti, L. Hao, The 2014 updated Draft PPWT: Hitting the spot or missing the mark?, *Space Policy*, 2015, 33, pp. 38–49.

98 United Nations, *Letter dated 12 February 2008 from the Permanent Representative of the Russian Federation and the Permanent Representative of China to the Conference on Disarmament Addressed to the Secretary-General of the Conference Transmitting the Russian and Chinese Texts of the Draft "Treaty on Prevention of the Placement Of Weapons in Outer Space and of the Threat or Use of Force Against Outer Space Objects (PPWT)*, UN Doc. CD/1839, p. 3.

99 United Nations, *Report by the Chair of the Group of Governmental Experts on further practical measures for the prevention of an arms race in outer space*, 2024, UN Doc. GE-PAROS/2024/CRP.1, p. 4.

populated with operational satellites and space debris. This situation raises the risk of collisions for both assets placed in LEO and launchers going through this orbit. In light of these challenges, considering space security in low Earth orbit is essential. To this end, space security is a "team sport" that requires coordination between different stakeholders. The private industry, and particularly space operators, have to invest in protective measures to mitigate risks of breaches and the number of vulnerabilities faced by space infrastructures. Commercial partners need to coordinate and exchange information on best practices within the supply chain and notify in case of unexpected malfunction or disruption and include resilient mechanisms to ensure the long-term sustainability of space missions. States also have an important role in fostering international cooperation and reducing tensions, while making sure national space activities are conducted in accordance with their international obligations. Here, diplomacy and the rule of law are important instruments to bolster space security and ensure the protection of the various activities carried out in low Earth orbit.

Bibliography

AFP, Smuggled Starlink dishes throw lifeline to some in war-torn Sudan, *France24*, 3 April 2024.

Aho, M., *United States Remarks for Conference on Disarmament Subsidiary Body 3—Prevention of An Arms Race in Outer Space*, Washington D.C., 22 March 2022. Available at: https://geneva.usmission.gov/2022/03/22/cd-prevention-of-an-arms-race-in-space/ (accessed: 02/02/2025).

Akcali Gur, B., **Kulesza, J.**, Equitable access to satellite broadband services: Challenges and opportunities for developing countries, *Telecommunications Policy*, 2024, 48(5), pp. 1–9.

Akcali Gur, B., **Kulesza, J.**, Satellite Internet Access in Times of Cyber Conflict, *Directions*, 28 April 2022.

Allahdadi, F.A., **Rongier, I.**, **Wilde, P.D.**, *Orbital Operations Safety*, [in:] *Safety Design for Space Operations*, Butterworth-Heinemann, Oxford 2013, pp. 411–415.

Australian Department of Infrastructure, Transport, Regional Development, Communications and the Arts, *Analysis of Low Earth Orbit Satellites*, Canberra 2024.

Azcárate Ortega, A., **Cesari, L.**, *The road to a moratorium on kinetic ASAT testing is paved with good intentions, but is it feasible?*, Fondation pour la Recherche Stratégique, Paris 2022.

Azcárate Ortega, A., **Samson, V. (eds.)**, *A Lexicon for Outer Space Security*, United Nations Institute for Disarmament Research, Geneva 2023.

Azcárate Ortega, A., **Samson, V.**, Counterspace Capabilities: Renewed Hope for Cooperative Governance?, *CIGI Papers*, 2025, 313.

Bailey, B., Cybersecurity Protections for Spacecraft: A Threat Based Approach, *The Aerospace Corporation*, 29 April 2021.

Bekkers, V., **Thaens, M.**, Interconnected networks and the governance of risk and trust, *Information Polity*, 2005, 10(1–2), pp. 37–48.

Boley, A.C., **Byers, M.**, Satellite mega-constellations create risks in Low Earth Orbit, the atmosphere and on Earth, *Scientific Reports*, 2021, 11(10642).

Britt, B., The PPWT and Ongoing Challenges to Arms Control in Space, *Joint Force Quarterly*, 2024, 113, pp. 81–85.

Casaril, F., **Galletta, L.**, Securing SatCom user segment: A study on cybersecurity challenges in view of IRIS2, *Computers & Security*, 2024, 140.

Centre for International Governance Innovation (Steer, C.), *International Humanitarian Law in the "Grey Zone" of Space and Cyber*, "A CIGI Essay Series Cybersecurity and Outer Space", Waterloo, Ontario 2023.

Cesari, L., *Commercial Space Operators on the Digital Battlefield*, „A CIGI Essay Series: Cybersecurity and Outer Space", Centre for International Governance Innovation, 29 January 2023.

Cheng, B., *Studies in International Law*, Clarendon Press, Oxford 1997.

Clark, J.B., *The Space Environment: An Overview*, [in:] L.R. Young, J.P. Sutton (eds.), *Handbook of Bioastronautics*, Springer, Cham 2021, pp. 23–57.

Clerc, P., Les enjeux juridiques de l'observation de la Terre depuis l'espace dans le contexte de la nouvelle économie spatiale, *Enjeux numériques*, 2024, 25.

Cory, N., **Dascoli, L.**, *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, Information Technology & Innovation Foundation, Washington D.C. 2021.

Cunningham, D.E., **Palavicini Jr., G.**, **Romero-Mariona, J.**, *Towards Effective Cybersecurity for Modular, Open Architecture Satellite Systems*, 30th Annual AIAA/USU Conference on Small Satellites, 21 July 2016.

Davalos, J., International Standards in Regulating Space Travel: Clarifying Ambiguities in the Commercial Era of Outer Space, *Emory International Law Review*, 2016, 30(4), pp. 610–611.

Denis, G., **Alary, D.**, **Pasco**, **X.**, **Pisot, N.**, **Texier, D.**, **Toulza, S.**, From new space to big space: How commercial space dream is becoming a reality, *Acta Astronautica*, 2020, 166, pp. 436, 440–443.

Erwin, S., Private satellite operators make case for helping military track ground targets, *SpaceNews*, 23 March 2024.

Evans, M., Overcoming Landing Rights Issues to Expand Access to Satellite, *Via Satellite*, 23 August 2024.

Eves, S., **Doucet, G.**, Reducing the civilian cost of military counterspace operations, *Humanitarian Law & Policy International Committee of the Red Cross*, 17 August 2023.

Feasey, R., **de Streel, A.**, **Alexiadis, P.**, **Bourreau, M.**, **Cave, M.**, **Godlovitch, I.**, **Manganelli, A.**, **Monti, G.**, **Shortall, T.**, **Timmers, P.**, *The Future of European*

Telecommunications: In-depth Analysis, Centre on Regulation in Europe, Brussels 2024, pp. 17–28.

Federal Communications Commission, *Order and Authorization DA 24-1193*, 26 November 2024.

Fortino, G., **Mastroianni, C.**, **Russo, W.**, Computer Systems Cooperative control of multicast-based streaming on-demand systems, *Future Generation Computer Systems*, 2005, 21(5), pp. 823–839.

Foust, J., GEO satellite operators seek multi-orbit strategies, *Space News*, 26 January 2022. Available at: https://spacenews.com/geo-satellite-operators-seek-multi-orbit-strategies/ (accessed: 02/02/2025).

Foust, J., SpaceX worked for weeks to begin Starlink service in Ukraine, *SpaceNews*, 8 March 2022.

Giannopapa, C., **Staveris-Poykalas, A.**, **Metallinos, S.**, Space as an enabler for sustainable digital transformation: The new space race and benefits for newcomers, *Acta Astronautica*, 2022, 198, pp. 728–732.

González Fanfalone, A., **Reisch, M.**, **Naito, M.**, **Lee, J.**, **Weber, V.**, Bridging connectivity divides, *OECD Going Digital Toolkit Notes*, 2021, 16, pp. 12–18.

Grey, R.T., Jr., Deadlocked and Waiting at the UN Conference on Disarmament, interview by Wade Boese, *Arms Control Today*, December 2000.

Grunert, J., The "Peaceful Use" of Outer Space?, *War on the Rocks*, 22 June 2021.

Hayes, A.D., **Caverly, R.J.**, Model predictive tracking of spacecraft deorbit trajectories using drag modulation, *Acta Astronautica*, 2023, 202, pp. 670–685.

Henry, C., Modernizing Manufacturing: How to Build the Satellite of the Future, *Via Satellite*, 30 March 2016.

Henry, E., Alleged Acquiescence Of The International Community To Revisionist Claims Of International Customary Law (With Special Reference To The Jus Contra Bellum Regime), *Melbourne Journal of International Law*, 2018, 18, pp. 10–11.

Hess, J., **Ley, B.**, **Ogonowski, C.**, **Wan, L.**, **Wulf, V.**, Understanding and supporting cross-platform usage in the living room, *Entertainment Computing*, 2012, 3(2), pp. 37–47.

Housen-Couriel, D., Cybersecurity threats to satellite communications: Towards a typology of state actor responses, *Acta Astronautica*, 2016, 128.

Hsieh, A., **Wu, V.**, Global maritime satellite market makes waves, *Digitimes Asia*, 11 December 2023.

International Law Commission, *Articles on the Responsibility of States for Internationally Wrongful Acts*, UN Doc. A/RES/56/83, Article 45.

International Regulatory Cooperation, *OECD Best Practice Principles for Regulatory Policy*, Organisation for Economic Co-operation and Development, Paris 2021.

International Telecommunication Union, *ITU-R: Managing the radio-frequency spectrum for the world*, August 2024.

International Telecommunication Union and the World Bank, *Overview of national spectrum licensing*, 6 October 2020.

Jameson, H., OTT: New Business Models Disrupting the Satellite Industry, *Via Satellite*, 24 July 2023.

Jang-Jaccard, J., **Nepal, S.**, A survey of emerging threats in cybersecurity, *Journal of Computer and System Sciences*, 2014, 80(5), pp. 974, 979.

Jiang, W., Software defined satellite networks: A survey, *Digital Communications and Networks*, 2023, 9(6), pp. 1243–1264.

Johnson, C.D., *The Legal Status of MegaLEO Constellations and Concerns About Appropriation of Large Swaths of Earth Orbit*, [in:] J. N. Pelton, S. Madry (eds.), *Handbook of Small Satellites*, Springer, Berlin 2020, pp. 1337–1339.

Jones, K., **Gordon, L.**, Global Communications Infrastructure: Undersea and Beyond, *The Aerospace Corporation*, 3 February 2022, pp. 7–8. Available at: https://csps.aerospace.org/papers/global-communications-infrastructure-undersea-and-beyond (accessed: 02/02/2025).

Kuskuvelis, I.I., The space risk and commercial space insurance, *Space Policy*, 1993, 9(2), pp. 109–120.

Latzer, M., **Just, N.**, **Saurwein, F.**, **Slominski, P.**, Institutional variety in communications regulation. Classification scheme and empirical evidence from Austria, *Telecommunications Policy*, 2006, 30(3–4), pp. 152–170.

Machi, V., *US Military Places a Bet on LEO for Space Security*, „Via Satellite", June 2021. Available at: https://www.sda.mil/us-military-places-a-bet-on-leo-for-space-security/ (accessed: 03/02/2025).

Magee, C., How the UK and NATO are preparing for spectre of nuclear war in space, *The I Paper*, 12 January 2025. Available at: https://inews.co.uk/news/world/uk-nato-preparing-spectre-nuclear-war-space-3470073?srsltid=AfmBOorx2FA8KE0BDqN9FJn4qMNOWNpAAeB9fGlqkoBKibtoKcVST-NZ9 (accessed: 02/02/2025).

Masson-Zwaan, T., **Hofmann, M.**, *Introduction to Space Law*, Kluwer Law International, Alphen aan den Rijn 2019.

McMahon, R., **Akcayir, M.**, **Norris, B.**, **Fabian, L.**, *Assessing the Impacts of Low-Earth Orbital Satellite Systems in Remote Indigenous Communities: Social and Economic Outcomes of Use in Northern Canada*, *Satellites and Beyond*, SSRN 2024. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5012799 (accessed: 02/02/2025).

Melamed, A., **Rao, A.**, **de Rohan Willner, O.**, **Kreps, S.**, Going to outer space with new space: The rise and consequences of evolving public-private partnerships, *Space Policy*, 2024, 68.

Merriam-Webster's Collegiate Dictionary, 11th ed., Merriam-Webster, Springfield, MA, 2025.

Mineiro, M.C., An inconvenient regulatory truth: Divergence in US and EU satellite export control policies on China, *Space Policy*, 2011, 27(4), pp. 213–215.

Nagelmackers-Voïnov, M., *Business and Private Diplomacy*, no. 3, Geneva Centre for Security Policy, Geneva 2017, pp. 2–4, 12.

OECD, Digital Security and Resilience in Critical Infrastructure and Essential Services, *OECD Digital Economy Papers*, 2019, 281, pp. 9–33.

Organisation for Economic Co-operation and Development, *Measuring the Internet of Things*, 13 October 2023, pp. 12–14.

Organisation for Economic Co-operation and Development, Satellite Communication: Structural Change and Competition, *OECD Digital Economy Papers*, 1995, 17, p. 15–16.

Paravano, A., **Rosseau, B.**, **Locatelli, G.**, **Weinzierl, M.**, **Trucco, P.**, Toward the LEO economy: A value assessment of commercial space stations for space and non-space users, *Acta Astronautica*, 2025, 228, pp. 453–455.

Pasco, X., *Enhancing Space Security in the Post Cold War Era: What Contribution from Europe?*, [in:] J.M. Logsdon, A.M. Schaffer, *Perspectives on Space Security*, Space Policy Institute, George Washington University, Washington D.C. 2005, pp. 51–68.

Pellegrino, M., **Stang, G.**, *Space security for Europe*, European Union Institute for Security Studies, Brussels 2016, p. 21–36.

Pelton, J.N., Defining a communications satellite policy system for the 21st century: A model for an international legal framework and a new "code of conduct", *Acta Astronautica*, 1996, 38(4–8), pp. 577–585.

Pelton, J., *Radio-Frequency Geo-location and Small Satellite Constellations* [in:] J.N. Pelton (ed.), *Handbook of Small Satellite*, Springer Reference, Cham 2020, pp. 1–13.

Poirier, C., The War in Ukraine from a Space Cybersecurity Perspective, *ESPI Short Report*, 2022, 1, pp. 1–25. Available at: https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Short-1-Final-Report.pdf (accessed: 03/02/2025).

Pratt, T., **Allnutt, J.E.**, *Satellite Communications, 3rd Edition*, Wiley-Blackwell, Hoboken, New Jersey 2019, pp. 543–633.

Rachfal, C.L., Low Earth Orbit Satellites: Potential to Address the Broadband Digital Divide, *Congressional Research Service Report*, 2021, R46896, pp. 6–12.

Rainbow, J., Dawn of the multi-orbit era, *SpaceNews*, 11 March 2024.

Rainbow, J., SpaceX gets conditional approval for direct-to-smartphone service, *SpaceNews*, 26 November 2024.

Raju, N., *Russia's anti-satellite test should lead to a multilateral ban*, Stockholm International Peace Research Institute, Stockholm 2021.

Raju, N., Space security governance: steps to limit the human costs of military operations in outer space, *Humanitarian Law & Policy International Committee of the Red Cross*, 22 August 2023.

Read, W.H., Network control in global communications, *Telecommunications Policy*, 1977, 1(2), pp. 125–137.

Reed, J., Leveraging LEO for Next-Generation In-Flight Connectivity, *Avionics International*, July/August 2023.

Regulation of NGSO Satellite Constellations, International Telecommunication Union and the World Bank, *Digital Regulation Platform*, 28 March 2024.

Rementeria, S., Power Dynamics in the Age of Space Commercialisation, *Space Policy*, 2022, 60.

République française, Ordonnance n° 2022–232 du 23 février 2022 relative à la protection des intérêts de la défense nationale dans la conduite des opérations spatiales et l'exploitation des données d'origine spatiale, *Journal officiel de la République française*, 2022, No. 0046.

Roberts, T.G., **Bullock, C.**, A sustainable geostationary space environment requires new norms of behavior, *MIT Science Policy Review. Communication*, 2020, 1, pp. 34–38.

Robinson, J., Transparency and confidence-building measures for space security, *Space Policy*, 2016, 37, pp. 134–144.

Roulette, J., Exclusive: Trump likely to axe space council after SpaceX lobbying, sources say, *Reuters*, 21 January 2025.

Saarikko, T., **Westergren, U.H.**, **Blomquist, T.**, The Internet of Things: Are you ready for what's coming?, *Business Horizons*, 2017, 60(5), pp. 667–676.

Sadiku, M.N.O., **Kotteti, C.M.M.**, **Sadiku, J.O.**, Information and Communication Technology: A Primer, *International Journal of Trend in Research and Development*, 2024, 11(3), pp. 171–174.

Salamatian, L., **Douzet, F.**, **Salamatian, K.**, **Limonier, K.**, The geopolitics behind the routes data travel, *Journal of Cybersecurity*, 2021, 7(1), pp. 1–19.

Sgobba, T., **Allahdadi, F.A.**, *Orbital Operations Safety*, [in:] F.A. Allahdadi, I. Rongier, P.D. Wilde (eds.), *Safety Design for Space Operations*, Butterworth-Heinemann, Oxford 2013, pp. 411–415.

Singh, K., **Psaledakis, D.**, U.S. Treasury says some satellite internet equipment can be exported to Iran, *Reuters*, 20 September 2022.

Sodders, L., *LEO, MEO or GEO? Diversifying orbits is not a one-size-fits-all mission (Part 1 of 3)*, US Space Operations Command, 18 July 2023.

Steer, C., *International Humanitarian Law in the "Grey Zone" of Space and Cyber*, "A CIGI Essay Series Cybersecurity and Outer Space", Centre for International Governance Innovation, Waterloo, Ontario 2023.

Steinbart, J., Problems and Issues in the Management of International Data Communications Networks: The Experiences of American Companies, *MIS Quarterly*, 1992, 16(1), pp. 55–76.

Su, J., The "peaceful purposes" principle in outer space and the Russia–China PPWT Proposal, *Space Policy*, 2010, 26(2), pp. 81–90.

Suomalainen, J., **Julku, J.**, **Vehkapera, M.**, **Posti, H.**, Securing Public Safety Communications on Commercial and Tactical 5G Networks, *IEEE Open Journal of the Communications Society*, 2 July 2021.

Tech State, Starlink Cracks Down on Unauthorized Roaming, Disconnects Users in Africa, *Tech Estate*, 16 April 2024.

Thales, Thales Seizes Control of ESA Demonstration Satellite in First Cybersecurity Exercise of its kind, *Thales Group*, 25 April 2023.

Tobias, A., **Leibrandt, W.**, **Fuchs, J.**, **Egurrola, A.**, Small satellites: Enabling operational disaster management systems, *Acta Astronautica*, 2000, 46(2–6), pp. 101–109.

Tronchetti, F., **Hao, L.**, The 2014 updated Draft PPWT: Hitting the spot or missing the mark?, *Space Policy*, 2015, 33, pp. 38–49.

Ullah, H., **Uzair, M.**, **Jan, Z.**, **Ullah, M.**, Integrating industry 4.0 technologies in defense manufacturing: Challenges, solutions, and potential opportunities, *Array*, 2024, 23, pp. 1–2.

United Nations Institute for Disarmament Research, *A Brief Overview of Norms Development in Outer Space*, Geneva 2012.

United Nations Office for Outer Space Affairs, *Guidelines for the Long-term Sustainability of Outer Space Activities of the Committee on the Peaceful Uses of Outer Space*, 2019, UN Doc. A/AC.105/118.

United Nations Office for Outer Space Affairs, *Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space*, 2007, UN Doc. A/62/20, Annex.

United Nations Secretary-General, *Secretary-General Urges Conference on Disarmament to Move Humanity Closer to Peace*, UN Doc. SG/SM/22139, 26 February 2024.

United Nations, *Constitution of the International Telecommunication Union*, adopted at the Additional Plenipotentiary Conference, as amended by subsequent plenipotentiary conferences, UNTS vol. 1002; *International Telecommunication Union, Guidelines for the Preparation of a National Table of Frequency Allocations (NTFA)*, Telecommunication Development Sector 2015.

United Nations, Convention on the Law of the Sea, Articles 87 and 112.

United Nations, *Group of Governmental Experts on Further Practical Measures for the Prevention of an Arms Race in Outer Space, Report of the Group of Governmental Experts on further practical measures for the prevention of an arms race in outer space*, 2024, UN Doc. GE-PAROS/2024/CRP.4.

United Nations, *Letter dated 12 February 2008 from the Permanent Representative of the Russian Federation and the Permanent Representative of China to the Conference on Disarmament Addressed to the Secretary-General of the Conference Transmitting the Russian and Chinese Texts of the Draft "Treaty on Prevention of the Placement Of Weapons in Outer Space and of the Threat or Use of Force Against Outer Space Objects (PPWT)*, UN Doc. CD/1839.

United Nations, *Recommendations on Possible Norms, Rules and Principles of Responsible Behaviors Relating to Threats by States to Space Systems*, submitted by the Federal Republic of Germany and the Republic of the Philippines, Open-ended Working Group on Reducing Space Threats through Norms, Rules and Principles of Responsible Behaviours, 2023, UN Doc. A/AC.294/2023/WP.1.

United Nations, *Report by the Chair of the Group of Governmental Experts on further practical measures for the prevention of an arms race in outer space*, 2024, UN Doc. GE-PAROS/2024/CRP.1.

United Nations, *Resolution adopted by the General Assembly on 7 December 2022 [on the report of the First Committee (A/77/383, para. 16)] 77/41, Destructive direct-ascent anti-satellite missile testing*, 2022, UN Doc. A/RES/77/41.

United Nations, *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)*, UNTS Vol. 610, No. 8843.

United Nations, *Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects (PPWT)*, 2002, UN Doc. CD/1579.

United Nations Secretary-General, *Secretary-General Urges Conference on Disarmament to Move Humanity Closer to Peace*, 2024, UN Doc. SG/SM/22139.

UNOOSA, *Registration of Objects Launched Into Outer Space, Stakeholder Study*, Vienna 2023.

Vernile, A., *The Rise of Private Actors in the Space Sector*, Springer, Berlin 2018.

Viscio, M.A., **Viola, N.**, **Fusaro, R.**, **Basso, V.**, Methodology for requirements definition of complex space missions and systems, *Acta Astronautica*, 2015, 114, pp. 80–81.

von der Dunk, F.G., Armed Conflicts in Outer Space: Which Law Applies?, *International Law Studies*, 2021, 188(97).

Wagner, E. Submarine cables and protections provided by the law of the sea, *Marine Policy*, 1995, 19(2), pp. 127–136.

West, J., **Miller, J.**, Clearing the Fog: The Grey Zones of Space Governance, *CIGI Papers*, 2023, 287.

White, C.L., Exploring the role of private-sector corporations in public diplomacy, *Public Relations Inquiry*, 2015, 4(3), pp. 305–321.

White House, The, *Remarks by Vice President Harris on the Ongoing Work to Establish Norms in Space*, 18 April 2022.

Wise, S., Eyes in the sky: The increasing importance of very low Earth orbit (VLEO) for national security, *SpaceNews*, 24 January 2024.

Wolf, J., Special report: The Pentagon's new cyber warriors, *Reuters*, 5 October 2010.

Zucherman, A.P., **Braun, B.M.**, **Sims, E.M.**, Space Safety Laws & Regulations: Navigating the policy compliance roadmap for small satellites, *Journal of Space Safety Engineering*, 2022, 9(4), pp. 582–599.

https://doi.org/10.18778/8331-719-9.08

Developing a Cybersecurity Policy for Low Earth Orbit Satellite Broadband: An International Law Perspective

Berna Akcali Gur[1]
Joanna Kulesza[2]

Introduction[3]

The demand for high-speed, low-latency connectivity is driving the rapid deployment of Low Earth Orbit (LEO) satellite constellations (LEOs). The LEOs are becoming integral to global Internet infrastructure to support the increasing need for broadband Internet access for social, economic, and governmental functions. LEOs can significantly reduce the digital divide by reaching underserved regions if utilised effectively. However, the cybersecurity threat landscape expanded by these systems remains a critical concern, with other significant interests—including digital inclusivity, digital autonomy, and data protection—posing obstacles to their effective deployment. Cybersecurity is fundamentally defined as the "security of cyberspace," which includes the complex web of connections and relationships among entities accessible through a generalized telecommunications network.[4]

1 Centre for Commercial Law Studies, Queen Mary University in London, United Kingdom and United Nations University – Institute on Comparative Regional Integration Studies, Brugge, Belgium.

2 Faculty of Law and Administration, University of Lodz, Poland.

3 This chapter is part of an Internet Society Foundation research project "Decolonizing the Internet: Global Governance of LEO-based satellite broadband."

4 ENISA, *Definition of Cybersecurity – Gaps and Overlaps in Standardisation*, Brussels 2015, p. 7. Available at: https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity_Definition_Gaps_v1_0.pdf (accessed: 31/12/2024).

It includes not only the objects themselves but also the interfaces that allow for remote control, data access, and participation in control actions within cyberspace. The reliance on satellite systems for broadband services is expected to grow significantly, thereby heightening these infrastructures' exposure to the existing cyber threat landscape. Also, the technologies used in LEOs create vulnerabilities that are unique to this technology. Furthermore, the anticipated integration of LEO satellites with new-generation mobile networks raises additional security concerns. New-generation wireless mobile technologies promise to drive industrial transformation and facilitate advanced mobile applications by delivering high speed and capacity for a wider range of applications low-latency, time-sensitive applications. This exponential increase in connected individuals, devices, organisations, and critical infrastructures underscores the need for robust cybersecurity measures, particularly given the international nature of satellite broadband.

LEOs, like all satellite systems, face a range of technical, natural, and manmade threats that can impact their operational security. Technical vulnerabilities, such as hardware failures and software glitches, can impair performance while increasing orbital congestion and kinetic threats, such as anti-satellite weapon tests, heighten environmental risks by generating orbital debris, potentially rendering the LEO unsafe for satellite use. Satellite systems are also vulnerable to electronic attacks like jamming and spoofing, alongside more traditional cyber threats targeting terrestrial infrastructure. National regulatory agencies and, most recently, the European Union Agency for Cybersecurity (ENISA) highlighted vulnerabilities within the unique ecosystem of LEOs. Indeed, the cybersecurity threats in LEOs have intensified concerns over domestic control and domestic protection of digital assets. As discussed by Roy Balleste and Laetitia Cesari in this Section, the LEOs become integral to global communications, the cybersecurity threat landscape, comprising the vulnerabilities inherent in Internet connectivity, expands. That is the reason for recent reviews of existing state oversight and security measures in light of this new infrastructure. The state authorities must ensure that security measures over cyber activities within their borders remain effective. These domestic measures, primarily adopted in response to growing global cyber security concerns, aim to mitigate risks associated with global interdependence but also reflect a desire to secure national interests in an interconnected digital world. Understanding this trend is essential to anticipate its implications for LEOs and their role in global connectivity.

Unlike other layers of the Internet, states regulatory oversight over telecommunications infrastructure within national borders has not been controversial. Consequently, the implementation of security measures in telecommunications has also been acceptable. The distinct characteristics of satellite broadband, which operates with minimal terrestrial infrastructure, present significant challenges to implementing some security measures. States seeking to leverage this complementary infrastructure often depend on a limited number of dominant providers. The substantial investment required for such initiatives, coupled with prohibitively high operational costs, diminishes their ability to deliver these services independently.

States express valid concerns regarding their reliance on infrastructure that is not fully understood or transparent, raising critical questions about national security and control. This raises questions about how existing domestic laws, traditionally applied to terrestrial infrastructure and Internet service providers, can be adapted for satellite services. While the international regulatory framework acknowledges providing satellite services only with appropriate domestic licensing and authorisation, implementing appropriate security measures remains challenging. The lack of a comprehensive international legal framework for cybersecurity, combined with geopolitical tensions—primarily driven by US-China rivalry—complicates global policy development. Implementing the right measures to address these cybersecurity challenges is essential to protect the growing role of LEOs in global connectivity. As noted by Mallory Knodell in Section IV of this book, global and regional multilateral and multi-stakeholder coordination, with the participation of countries relying on LEOs', that aligns with international law and Internet governance frameworks would produce the best solutions. However, in the current climate, these processes are unlikely to produce results in time. In the meantime, the domestic authorities will be compelled to act to benefit from LEOs.

This paper discusses potential domestic policy options considering the cybersecurity risks associated with LEOs. The second section introduces basic LEO architecture and its role in global Internet infrastructure. The second section introduces cybersecurity risks associated with LEOs with reference to recent reports and regulatory changes. The fourth section introduces the significance of multistakeholder processes for global cybersecurity efforts. The fifth section introduces a matrix of potential policy options and their impact on cybersecurity. The sixth section concludes.

Basic architecture of LEO satellite broadband systems

To effectively inform policy decisions and regulatory frameworks concerning LEOs, it is essential to grasp their basic architecture. This section provides a concise overview. LEO refers to the orbital zone between 300 and 2,000 kilometres above the Earth. It is used for various satellite services, including communications, Earth observation, and scientific research. The proximity of satellites in LEO allows for significantly shorter signal transmission times compared to Medium Earth Orbit (MEO) and Geostationary Orbit (GEO) systems. MEO is the orbital zone between LEO and GEO -the traditional location for communications satellites at 35,786 kilometres. When used for broadband Internet services, the proximity LEOs enable high-speed, low-latency services compatible with contemporary terrestrial networks, primarily consisting of wireless mobile networks and fibre optic cables. Low latency is particularly critical for real-time applications such

as industrial process controls, navigation, and video games. The LEOs have also started leveraging the strengths of different orbits to provide enhanced connectivity and resilience. The number of hybrid network architectures in operation that combine LEOs with higher altitude satellites in MEO and GEO is increasing.

Satellite constellations consist of multiple identical or similar satellites designed to operate as a network through shared control for a shared purpose. The lower altitude of satellites deployed in LEO results in each one covering a smaller geographical area, necessitating the deployment of constellation systems consisting of larger numbers to achieve global coverage—unlike the three in GEO or six in MEO. In response to the exponential increase in number of satellite filings for increasing number of LEOs, the International Telecommunication Union (ITU) updated its regulations in 2019 to define LEOs as non-geostationary satellite systems "having more than one orbital plane where mutual relative position of each orbital plane and mutual relative position of each satellite in its orbital plane is important".[5] Each satellite's position is vital to the LEOs' functionality as they move along pre-planned trajectories facilitated by both ground coordination and inter-satellite links. Typically composed of smaller, more affordable satellites that are produced in large numbers and are launched in multiple numbers. Therefore, LEOs are easier to expand and renew when compared to bigger, custom-made satellites at higher altitudes. As the number of satellites in LEO increases, sophisticated international space traffic management becomes essential to ensure the security and sustainable use of the LEO or the infrastructure it hosts. These challenges impact space-faring nations with assets in orbit and also those reliant on their satellite services. At the international level, the shared use of Earth's orbits is governed by international telecommunications regulations and outer space law, which are subbranches of international law.

The LEOs comprise three segments: ground, space and the user segment. All satellites require ground stations (gateways) to communicate with the Earth. For broadband services, these are necessary to transmit data between satellites and the terrestrial Internet backbone. They are intermediaries relaying data and managing network traffic. As of writing, stations must be no more than 1,000 kilometres apart for global service provision. However, reliance on ground stations is expected to decline as inter-satellite links improve.[6] There are various ways in which satellite broadband services could utilised. In the basic direct-to-consumer business model, consumers need user terminals provided by the satellite service provider to connect their internet-enabled devices. The user terminals will link to the nearest satellite, while several other satellites in the constellation will maintain connection to the ground stations. The setting up of ground stations and the importation of user terminals are subject to the regulations of the jurisdictions they are located in and/or exported to. The domestic

5 WRC-19, mandatory data item A.4.b.1.a of Appendix 4 – a.

6 *Starlink*. Available at: https://www.starlink.com/business/direct-to-cell (accessed: 25/07/2025).

regulatory authorities determine licensing and authorisation requirements for both, which gives them leverage to regulate according to their own specific needs.

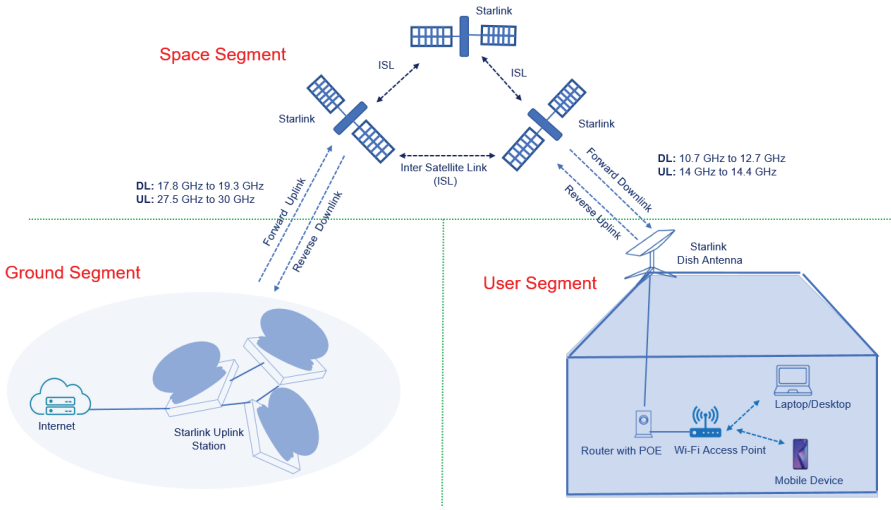


Fig. 1. A diagram of the key features of a satellite broadband system
Source: SpaceX – Starlink System Architecture for Internet, *Techplayon*, 12 January, 2024. Available at https://www.techplayon.com/starlink-system-architecture/ (accessed: 31/12/2024).

Additionally, the frequency spectrum allocation is essential for uplink and downlink connections between satellites and user terminals or ground stations. The ITU manages global frequency spectrum coordination and associated orbit resources, both finite resources, and ensures their efficient and equitable use. Domestic regulators assign frequencies within their borders through licensing processes. These assignments comply with ITU coordination to avoid interference with other countries' services. Continuous provision of all wireless communication services, including satellite services, requires interference-free access to an allocated frequency spectrum.[7] Therefore, it is a key issue when discussing all matters concerning LEOs, including their cybersecurity.[8] Dan York provides a detailed analysis on the architecture of LEOs in his chapter.

7 See also: D. Voelsen, Internet from Space, *Stiftung Wissenschaft und Politik Research Paper*, 2021, 6. Available at: https://www.swp-berlin.org/en/publication/satellite-internet (accessed: 24/02/2025); Internet Society, *Perspectives on LEO Satellites*, Massachusetts 2022. Available at: https://www.internetsociety.org/resources/doc/2022/perspectives-on-leo-satellites/ (accessed: 31/12/2024).

8 J. Manner, *Spectrum Wars: The Rise of 5G and Beyond*, Artech House, Virginia 2021.

LEOs and the global Internet infrastructure

The Internet is primarily delivered through terrestrial infrastructure. However, when terrestrial networks are impractical or unavailable during emergencies, satellites have been a crucial last-mile solution in remote and sparsely populated areas, on land, at sea, and in the air. Despite the much-improved speed and latency of LEOs, satellite broadband is not viewed as a replacement for terrestrial infrastructure, which primarily relies on fibre-based networks that provide reliable, interference-free data transmission at light speed.

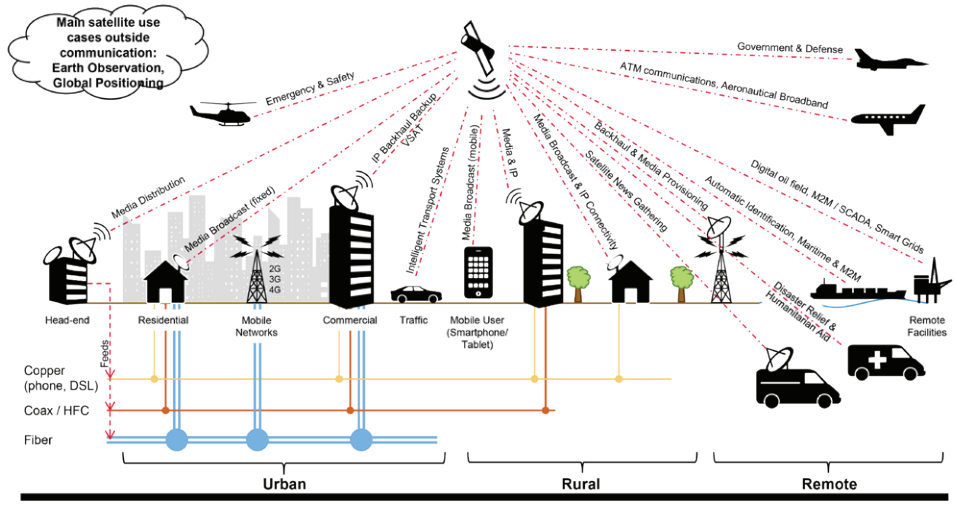


Fig. 2. Satellites' role in the global internet infrastructure
Source: S. Raman, R. Weigel, T. Lee, The Internet of Space (IoS): A Future Backbone for the Internet of Things?, *IEEE Internet of Things*, 8 March 2016. Available at: https://iot.ieee.org/articles-publications/newsletter/march-2016/the-internet-of-space-ios-a-future-backbone-for-the-internet-of-things.html (accessed: 31/12/2024).

The advancement of wireless mobile technologies has increased the significance of cybersecurity for the resilient and secure provision of social, commercial, and governmental internet-enabled functions. Before the emergence of large LEO constellations, it was believed that satellites would have a limited role in global Internet infrastructure. Their future market share remains uncertain, with some companies now incorporating smaller LEO constellations into their existing MEO and GEO satellite networks to remain competitive.[9] Diverse business models have

9 S. Waterman, Beyond GEO: Major Operators Have A Multi-Orbit Focus, *Viasatellite*, 12 March 2020. Available at: https://interactive.satellitetoday.com/beyond-geo-major-operators-have-a-multi-orbit-focus/ (accessed: 31/12/2024).

already emerged. Starlink's primary focus is a direct-to-consumer model, and EUTELSAT OneWeb and Hughes Network Systems focused on business-to-business and business-to-government services, providing backhaul for wireless communications and serving as backups to fibre-optic networks. Ultimately, satellite broadband technology is likely to complement the global communications landscape rather than replace existing cable and wireless infrastructures. As the market matures and use cases increase, authorities and technical experts are gaining a deeper understanding of the cybersecurity challenges specific to satellite broadband.

Cybersecurity of LEOs

The main policy challenge at the intersection of LEO satellite broadband and its cybersecurity access stems directly from the history of telecommunications infrastructure development. The Internet has been developed by industrialized societies and still largely relies on infrastructure and applications built, operated, and owned by them. The imbalanced ownership structure empowers the already powerful while sustaining the gap between them and the others. Over the years, the global inequity in sharing the benefits of Internet technologies and infrastructure has remained. The dependence and use of non-domestic infrastructure and applications and cross-border data transfers have come to be assessed concerning their national security, cybersecurity and economic security risks. A recent relevant high-profile example was the cyberattack by Russia on ViaSat, impacting thousands of users and internet-connected wind farms across central Europe when targeting Ukraine's military communications. It remains uncertain whether the spillover effects of this incident were intentional. As exemplified in this incident, the protection of Internet networks is linked to national and regional security. Despite their concerns, countries continue their best efforts to invest in and acquire technology and infrastructure that will facilitate their digital transformation, which is essential to meet developmental steps. If LEOs are to play a significant role in that endeavour by speeding up the process by which broadband Internet is made available, cybersecurity concerns need to be assessed and addressed.

Recognising the urgency of the issue, the European Union Agency for the Space Programme (EUSPA) has conducted a study on the security of space communication technologies. Their report found that the proliferation of software-defined satellite systems' use in global data transfers, the reliance on in-orbit reconfigurations, and adopting laser-based data transfer methods exacerbate cyber security vulnerabilities.[10] This study justifies investment in a European Union (EU) controlled autonomous LEO satellite constellation. Before that, the United States (US) Space Policy Directive-5, signed in 2020, established key cybersecurity principles for space systems to ensure they are resilient to cyber incidents and radio-frequency

10 European Commission, EUSPA, *The Secure SATCOM Market and User Technology*, Brussels 2023.

spectrum interference. This directive sets forth a comprehensive, standards-based approach focusing on supply chain security, encryption, and physical component security. The Satellite Cybersecurity Act, which would require the Cybersecurity and Infrastructure Security Agency to consolidate voluntary satellite cybersecurity recommendations to help companies understand how to secure their systems best, was introduced in Congress in 2022 but has not been adopted as of the date of this article.[11] Also, while the communication and information technology sectors are already categorised as critical infrastructures in the US, space systems have not received similar recognition. There are ongoing discussions as to whether this should change.[12] The United Kingdom's (UK) Space Industry Regulations, enacted in 2021, also include a dedicated section on cybersecurity. Accordingly, the applicants should have a cybersecurity strategy for their proposed operation based on a security risk assessment. Licensees must also maintain a cybersecurity strategy for their network and information systems. These regulations are complemented by the Telecommunications (Security) Act of 2021, which imposes stringent security requirements on public telecommunications providers, including those operating satellite communications (satcom).[13] The EU has also recognised the urgency of addressing cybersecurity in space communications through its recently passed Network and Information Systems Directive, and further regulated the security aspects of space-based services under the CER Directive. The UK and EU initiatives are particularly relevant for developing nations. They include parts that specifically focus on non-domestic services—an issue that resonates with developing nations that similarly rely on foreign technologies. Also, they possess insights and expertise in space technologies due to their long-time space-faring activities. The EU, especially, has successfully influenced global regulatory developments, and it is likely to continue that role in shaping space regulations.

These regulatory updates highlight the recognition of the changing cyber threat landscape associated with space communications technologies. The approaches taken by the US, UK, and EU suggest that commercial entities providing broadband services will face scrutiny not only regarding their cybersecurity vulnerabilities but also concerning the risks they pose as components of domestic infrastructure. The main reason is that LEOs, like all Internet systems are inherently exposed to threats that exploit existing vulnerabilities. The specific malicious threats targeting LEOs compound these vulnerabilities and are crucial for developing effective prevention and recovery strategies. These include cyber-attacks, which encompass a range of

11 E. Graham, Lawmakers Reintroduce Legislation to Bolster Satellite Cybersecurity, *NextGov*, 4 May 2023. Available at: https://www.nextgov.com/cybersecurity/2023/05/lawmakers-reintroduce-legislation-bolster-satellite-cybersecurity/385991/ (accessed: 31/12/2024).

12 E. Swallow, S. Visner, It's time to declare space systems as critical infrastructure, *Politico*, 2 April 2021. Available at: https://www.politico.com/news/2021/04/02/its-time-to-declare-space-systems-as-critical-infrastructure-478848 (accessed: 31/12/2024).

13 OFCOM, *Wider regulatory obligations*, 30 January 2023. Available at: https://www.ofcom.org.uk/spectrum/space-and-satellites/wider-regulatory-obligations (accessed: 31/12/2024).

activities such as data breaches, denial-of-service attacks, and other forms of network intrusion aimed at compromising system integrity and availability. Physical security threats, such as sabotage or destruction of ground facilities, satellite assets, or associated infrastructure.[14] The risks posed by insiders also deserve attention. Employees or contractors with access to sensitive systems may intentionally or unintentionally compromise system security. Supply chain vulnerabilities can further complicate the scenario, as weaknesses in the supply chain can be exploited, impacting the quality and security of satellite components and systems. Moreover, state-sponsored or organised crime groups may target satellite broadband systems to obtain sensitive information or disrupt services.

Technical risks facing LEO satcom systems are multifaceted and often interconnected. For instance, user service degradation or outright outages can compromise the quality of services offered, leading to diminished throughput or even total service interruptions.[15] Similarly, the monitoring and control capabilities of the system may degrade, resulting in a loss of command over the spacecraft or the associated ground segments. These failures can have cascading effects, such as asset damage or destruction, which might result from incidents like overdriving an onboard analog-to-digital converter with excessively strong radio frequency signals.[16] Moreover, the disclosure of sensitive information, such as spacecraft engineering blueprints, poses a significant risk through data theft or leaks. External factors can also contribute to vulnerabilities; for example, damage to service quality due to interference affecting a neighbouring satellite resulting from damage to or theft of services or assets belonging to external organisations. Capability hijacking further complicates the landscape, allowing unauthorised use of a satellite's capabilities, including its communication systems. Additionally, the risk of data interference threatens the operational integrity of the entire system.

Another important issue is that the LEOs are complex technological infrastructures with substantial financial implications. From a business perspective, financial and commercial risks in the satellite broadband market can impact on the tangible and intangible assets of all organisations involved, such as their reputation and profitability. Disruptions to earth, space or user components of satellite systems can hinder satellite broadband service delivery and have financial repercussions. Poor performance can significantly damage the credibility of service providers and their partners. In addition to service delivery issues, satellite broadband services often operate under service-level agreements (SLAs), which are agreements between a satellite service provider and a customer. The SLAs outline the services to be provided and the standards the provider must meet. Failure to meet SLA requirements, particularly when satellite broadband is a backup for

14 European Union Agency for Cybersecurity (ENISA), *LEO Satcom Cybersecurity Assessment*, Brussels 2024, p. 23. Available at: https://www.enisa.europa.eu/publications/low-earth-orbit-leo-satcom-cybersecurity-assessment (accessed: 31/12/2024).

15 *Ibidem*.

16 *Ibidem*, p. 22 ff.

terrestrial services, can lead to financial penalties. The re-emergence of geo-political and geo-economic competition in space. The high-stakes nature of investments in LEOs makes securing reliable debt financing challenging; the perfect stage for enhanced public-private partnerships with a leading role in the state.[17] Today, the connection between public and private actors remains strong, impacting how third countries perceive cyber threats. This viewpoint aligns with the arguments presented in Monica Stachon's chapter. To see beyond these geo-political dynamics relies on developing expertise to adopt a fact-based approach in developing comprehensive cybersecurity strategies and addressing potential threats through robust prevention measures and responsive recovery plans.

Should governments fail to recognize the significance of this contemporary challenge, they will be deemed to rely on the circumstantial status quo resulting from the current, uninhibited competition by companies among major global powers. A few commercial actors and their home states will shape the policy discourse and the cybersecurity standards. Bearing in mind that the satellite broadband companies provide services across borders, they are subject to laws and regulations of not only their home jurisdictions but also of the jurisdictions in which they provide their services, all of which would have been developed in compliance with the relevant international treaties, especially on telecommunications and trade. Regulators of third states could leverage their jurisdictional rights and relevant multilateral platforms to ensure their cybersecurity concerns are addressed. Examples of this dynamic are explored in Section III by Célestine R. Rabouam, Monika Stachoń and Jason Bonsall. Following and engaging in current policy debates within the ITU, WTO, and the UN, as well as regional policy and economic forums.[18] If they lack the resources to engage in these platforms effectively and to make effective, informed decisions about LEOs and the appropriate cybersecurity measures, pooling their resources and operational and technical expertise with other actors who share similar concerns should be part of their cybersecurity policy development.

Multistakeholderism and Cybersecurity Policy for LEOs

Domestic authorities should have due regard to the current multistakeholder model of Internet governance and policy protocol development, which might impact national legislative action for LEOs and their cybersecurity. With its current regulatory design, the Internet is intentionally decentralized to effectively defer threats to the network and its resources; there is no single point of control that,

17 European Commission, *The Future of European Competitiveness: Part B – In-depth Analysis and Recommendations*, Brussels 2024, p. 173 ff. Available at: https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en/ (accessed: 31/12/2024).

18 See also: R.H. Weber, Regulatory Autonomy and Privacy Standards under the GATS, *Asian Journal of WTO & International Health Law & Policy*, 2012, 7, p. 25.

if compromised, could disable the entire global network. This reflects the original network design goal of creating a global communication system resistant to a single, likely nuclear, attack. This decentralized design was founded on dispersed infrastructure (local software and network backbone architecture) and a democratic, peer-to-peer model of cooperation and trust. All network nodes have equal status, and their efficient operation is dependent on trust in other actors—trust has always been the oil of the global digital economy. This egalitarian, dispersed model differed significantly from other known governance models—whether public or private, networks and communities are based on authority, power, and enforcement. Despite lacking both, the Internet continued to function, and its governance model quickly proved critical to its success. In 2003, ITU member states recognized its social, economic, and political potential. The 2003 World Summit on the Information Society (WSIS), hosted by the ITU in Geneva, was the first official intergovernmental meeting to address the opportunities and challenges that the global network presents to international and domestic policies. It established the Working Group on Internet Governance (WGIG), a small group of telecommunications and international relations professionals appointed by member states, to identify the initial challenges and potential solutions posed by this global communication phenomenon to international policies. In 2005, the WGIG issued a report that defined "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.[19]

This definition reflects the wide range of standard-setting and decision-making bodies and processes critical to the global network's day-to-day operation. It also expresses the fundamental principle of Internet governance: the multistakeholder principle. While "multi-stakeholderism" is widely used in international relations theory and practice, official UN documents frequently refer to a "multistakeholder approach" to Internet governance. The Tunis Agenda also emphasizes the importance of the multistakeholder approach as a means to "improve coordination of the activities of international and intergovernmental organizations and other institutions concerned with Internet Governance, as well as an information exchange among themselves."[20] The principle of multistakeholder governance has also been recognized in the context of online human rights protection, as evidenced by the Council of Europe (CoE) 2011 Declaration of the Committee of Ministers on Internet Governance Principles, in which the ministers refer to "multistakeholder governance." The CoE recommends "the development and implementation of Internet

19 World Summit on the Information Society, *Tunis Agenda for the Information Society*, WSIS-05/TUNIS/DOC/6(Rev. 1), 18 November 2005. Available at: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html (accessed: 25/07/2025).

20 *Ibidem*.

governance arrangements" in a way that ensures "the full participation of governments, the private sector, civil society, the technical community, and users, taking into account their specific roles and responsibilities, in an open, transparent, and accountable manner."[21] The document emphasizes two aspects of multistakeholder governance: equal representation from all community sectors and geographic regions. Regarding network integrity, the CoE ministers cite "security, stability, robustness, and resilience of the Internet" as "key objectives" of Internet governance. This goal will be accomplished through "national and international multistakeholder collaboration" to preserve "the integrity and ongoing operation of the Internet infrastructure, as well as users' trust and reliance on the Internet." The post-WSIS decade (2005–2015) fueled discussions on specifying the ambiguous notion of "Internet governance," most significantly through defining the "respective roles" of states, businesses, and civil society. Considering all these challenges that come with the multistakeholder model of Internet governance, this intended distribution of competencies among three groups of relevant stakeholders suggests that Internet governance remains the most viable and recommended policy option for the stable and secure management of critical Internet resources.

An alternative solution would be splitting the global network into smaller, national, or regional intranets managed by national authorities or regional intergovernmental organisations. This argument is usually part of the eagerly unfolding "splinternet" debate. Theoretically, a local or regional network based on fully controlled infrastructure and protocols might provide a lesser regulatory challenge and be easier to secure. Some countries and regions have indeed pursued this policy objective, such as the Great Chinese Firewall, the more recent Russian RuNet project, or the latest EU draft policy on DNS4EU. However, a policy option to develop a national network that is fully controllable, secure, and independent is not recommended for both operational and economic reasons. From a global development perspective, dividing the global network would deprive the Internet of being an enabler for sustainable growth, innovation, and access to knowledge. If a state were to consider this policy option for LEOs and attempt to establish fully independent domestic critical infrastructures which will include LEOs, such an endeavour would likely prove technically challenging, costly, and detrimental to that country's developmental capacity.[22]

The recent adoption of the Global Digital Compact marks a significant milestone in international efforts to establish an open, safe, and secure digital future for all. Led by Sweden and Zambia, this intergovernmental process involved extensive consultations with Member States and stakeholders from January to June 2023. The Compact's adoption by world leaders on 22 September 2024 at the Summit of the Future underscores a collective commitment to multistakeholder governance

21 *Ibidem*.

22 *The Internet and Sustainable Development – Internet Society*. Internet Society, Virginia 2015. Available at: https://www.internetsociety.org/resources/doc/2015/the-internet-and-sustainable-development (accessed: 31/12/2024).

in cyberspace. This initiative reaffirms the essential role of diverse stakeholders—governments, the private sector, civil society, and technical communities—in shaping a resilient and inclusive digital landscape. By prioritising collaboration, the Global Digital Compact reinforces the multistakeholder model as a foundational framework for addressing contemporary challenges in global digital governance. In this context, the policy matrix presented below complements the objectives of the Global Digital Compact by offering actionable strategies for national authorities, businesses, and internet end users.

Multistakeholderism plays a crucial role in enhancing cybersecurity including cybersecurity of satellite broadband networks, where diverse interests and expertise converge. The multifaceted nature of cyber threats necessitates collaboration among various stakeholders, including governments, private sector entities, civil society, and technical communities. By engaging multiple stakeholders in cybersecurity discussions, the potential for more innovative and effective solutions increases. Each stakeholder brings unique insights and resources that contribute to a more nuanced understanding of the cybersecurity landscape. For instance, private LEO companies have firsthand experience with emerging threats and can provide practical insights into the implementation of security measures. Meanwhile, governmental authorities can offer insights into the implications of alternative regulatory frameworks and resources for broader strategic initiatives.

Moreover, multistakeholder engagement fosters transparency and accountability in the development and implementation of cybersecurity policies. When stakeholders collaborate in policy-making processes, they can collectively address concerns regarding procedural fairness and equitable benefit distribution. This inclusivity not only enhances trust among stakeholders but also encourages a shared sense of responsibility for the security of the digital environment. In LEOs where vulnerabilities can have far-reaching implications, multistakeholderism becomes even more essential. The complex interdependencies inherent in satellite systems necessitate a coordinated approach to cybersecurity that encompasses not just the technology itself but also the broader regulatory and operational frameworks that govern its use. By leveraging the strengths of various stakeholders, it is possible to develop more robust cybersecurity measures that protect against both technical failures and malicious attacks.

Ultimately, the integration of multistakeholder principles into cybersecurity efforts supports a resilient digital infrastructure that is better equipped to withstand and respond to emerging threats to LEOs. As the landscape of LEO cybersecurity continues to evolve, fostering collaboration among diverse stakeholders will be key to achieving a secure and sustainable digital future.

Six LEOs policy options

An effective domestic policy intervention must ensure cybersecurity interests and take due regard to the interests of other stakeholders. It should, therefore, include a thorough understanding of technical operations behind LEO satellite-based broadband access, a dedicated analysis of competing economic interests and available services, including a security risk assessment for the supply chain and ensuring fair market access to all service providers and consumers, with due regard to the interests of developing countries; prioritising existing economic interests of leading commercial actors might negatively impact those of up-and-coming entrepreneurs from non-space-faring countries. Moreover, it must include revising or developing legislation to ensure the application of fundamental rights protection for all individual Internet end users, in particular, the right to privacy.

The current policy and legal framework enables the identification of six potential policy options that stakeholders consider when developing their LEO satellite broadband strategies. Each option carries distinct implications for the cybersecurity of LEOs. A matrix outlining these policy options is provided, as shown in their descriptions below.

Tab. 1. LEOs regulation policy options

OPTION	APPROACH	KEYWORD	DESCRIPTION
OPTION 1	**EFFICIENT**	**„QUICK LEOs"**	PROMPTLY ALLOW NATIONAL LEO SATELLITE BASED INTERNET ACCESS
OPTION 2	**CAUTIOUS**	**„SLOW LEOs"**	DEVELOP GUIDING POLICY QUESTIONS TO CONSIDER BEFORE DECIDING ON LEO SATELLITES BASED SERVICE IN YOUR JURISDICTION
OPTION 3	**PASSIVE**	**„NO LEOs"**	REFRAIN FROM ALLOWING LEO SATELLITE BASED SERVICE WITHIN YOUR JURISDICTION, CAUTIOUSLY OBSERVE FURTHER DEVELOPMENT, WAIT FOR THE TECHNOLOGY TO MATURE
OPTION 4	**COST-INTENSIVE**	**„MY LEOs"**	DEVELOP NATIONAL/REGIONAL LEO SATELITES BASED BROADBAND SERVICE
OPTION 5	**COOPERATIVE**	**„OUR LEOs"**	JOIN FORCES WITH LIKE MINDED ACTORS TO DEVELOP A COMPREHENSIVE, RULES BASED ORDER FOR LEO BASED ACCESS, FACILITATING GLOBAL ACCESS AND CONNECTMTY FOR ALL THROUGH SUSTAINABLE DEVELOPMENT GOALS

OPTION	APPROACH	KEYWORD	DESCRIPTION
OPTION 6	**ENGAGED**	**„UNIVERSAL LEOs"**	ACTIVELY ENGAGED WITHIN EXISTING INTERNATIONAL AND REGIONAL FORUMS TO ENSURE RELEVANT POLICIES CURRENTLY DEVELOPED FACILITATE GLOBAL ACCESS AND CONNECTMTY FOR ALL THROUGH SUSTAINABLE DEVELOPMENT GOALS

Source: authors' own work.

The efficient approach, referred to as "Quick LEOs" in the above table, posits that LEO satellite-based broadband Internet access is the state's foremost priority. This option emphasises rapid availability to underserved regions, placing greater importance on immediate access than on potential concerns regarding national security, cybersecurity, or privacy. Governments adopting this model favour authorising already operational service providers, enabling swift Internet access upon license approval. This approach yields immediate benefits, including a rapid increase in Internet availability that fosters growth and innovation. The authorities trust the cybersecurity standards implemented by the service provider and the existing domestic cybersecurity measures in place. In this policy choice, if LEOs' specific data security and liability risks are not adequately addressed by the existing regulatory framework, public and private organisations and individual users may suffer when threats actualise. This policy option is particularly risky for non-space-faring nations, which are less likely to have the expertise to have an already existing effective cybersecurity framework in place.

The cautious approach, termed "Slow LEOs," encourages governing authorities to formulate guiding policy questions, including for cybersecurity, before committing to satellite broadband services within their jurisdiction. In this policy alternative, authorities promote informed decision-making. They are recognised as a hallmark of good governance, but they inevitably delay the expansion of Internet access and are resource and time-consuming.

The passive option, which we refer to as "No LEOs," entails a complete abstention from permitting satellite broadband services. States that adopt this stance opt to monitor technological advancements, allowing cybersecurity measures to mature before making any decisions. While this strategy minimises immediate risks and liabilities, including those linked to cybersecurity, it can also delay innovation and growth linked to connectivity, potentially hindering economic and developmental progress. Consequently, the passive approach is not advisable, especially if there is an urgent need to address connectivity gaps.

The cost and resource-intensive "My LEOs" option signifies that the governing state intends to establish its own LEOs and cybersecurity standards, thereby achieving full technological autonomy. This approach guarantees

complete control over security measures by eliminating reliance on third-party infrastructures. While developing its satellite capabilities may yield substantial security benefits, this strategy is resource-intensive, and delays in project deployment may delay the receipt of the associated connectivity benefits. These delays may inhibit targeted enhancements in Internet penetration or competitive advantages. Moreover, it may not provide protection from global cyber threats inherent in the global Internet networks, and it may stifle international cooperation. This option is only available to countries with financial and technical resources to establish a LEO constellation. It could emerge in the way that the EU has done, authorising foreign companies yet planning an EU-based system for governmental purposes, or as in the China model, which plans only to authorise China-based LEOs.

The cooperative approach, referred to as "Our LEOs," encourages like-minded states to collaborate in formulating comprehensive, transparent, rules-based policies and cybersecurity standards for LEO broadband access. This option promotes the use of LEOs controlled and operated by trusted partners. However, adopting this approach demands significant resources for continued collaboration, including human capital, capacity building, and active community involvement in multistakeholder platforms. Given its capacity to facilitate a secure and sustainable development framework for LEO satellite broadband, this option is desirable. Yet, countries that suffer most from the connectivity gap may lack the resources to participate actively in the processes where decisions are made.

Lastly, "Universal LEOs" builds upon the cooperative model by striving for active engagement with existing international and regional forums. It seeks to ensure that relevant policies facilitate global connectivity for all. This option promotes the efficient use of LEOs through equitable benefit sharing and aims to enhance global connectivity for sustainable development. These forums can range from various UN specialised agencies to other multilateral and multistakeholder organisations such as the ICANN, and IGF, as well as technical or academic platforms working on satellite broadband developments. However, adopting this approach requires strong political will and significant resources for ongoing collaboration, including human capital, capacity building, and active community involvement. Nevertheless, it presents the opportunity to establish a sustainable and secure policy for LEO satellite broadband cybersecurity, which justifies the associated costs and should, therefore, be strongly recommended. Despite its potential to create a sustainable development framework for LEO satellite broadband, this option is the most desirable and least likely to be realised.

Tab. 2. LEO policy options with recommendations

OPTION	APPROACH	KEYWORD	DESCRIPTION	STRENGTHS	LIMITATIONS	RECOMMENDATION
OPTION 1	EFFICIENT	"QUICK LEOs"	PROMPTLY ALLOW NATIONAL LEO SATELLITE-BASED INTERNET ACCESS	INSTANT INCREASE IN INTERNET PENETRATION POPULAR APPROACH AMONG NON-SPACE-FARING NATIONS FACILITATES GROWTH AND INNOVATION	POTENTIAL DATA SECURITY AND LIABILITY RISKS FOR STATE AND INDIVIDUAL USERS UNPOPULAR APPROACH AMONG SPACE-FARING NATIONS	NOT RECOMMENDED
OPTION 2	CAUTIOUS	"SLOW LEOs"	DEVELOP GUIDING POLICY QUESTIONS TO CONSIDER BEFORE DECIDING ON LEO SATELLITES BASED SERVICE IN YOUR JURISDICTION	ALLOWS FOR INFORMED DECISION MAKING GOOD GOVERNANCE PRACTICE	TIME CONSUMING DELAYS PENETRATION INCREASE	RECOMMENDED
OPTION 3	PASSIVE	"NO LEOs"	REFRAIN FROM ALLOWING LEO SERVICE; OBSERVE DEVELOPMENT AND WAIT FOR TECHNOLOGY TO MATURE	UPHELD STATUS QUO: NO RISK OR NEW LIABILITIES	PERMANENTLY STIFFLES INNOVATION AND GROWTH	NOT RECOMMENDED
OPTION 4	COST-INTENSIVE	"MY LEOs"	DEVELOP NATIONAL/REGIONAL LEO SATELLITE-BASED BROADBAND SERVICE	FULL TECHNOLOGICAL AUTONOMY / INDEPENDENCE	EXTREMELY COST-INTENSIVE DELAYED RESULTS: NO IMMEDIATE INTERNET PENETRATION GROWTH STIFFLES INTERNATIONAL COOPERATION	NOT RECOMMENDED

Tab. 2 (cont.)

OPTION	APPROACH	KEYWORD	DESCRIPTION	STRENGTHS	LIMITATIONS	RECOMMENDATION
OPTION 5	COOPERATIVE	"OUR LEOs"	COLLABORATE WITH LIKE-MINDED ACTORS TO ESTABLISH A COMPREHENSIVE, RULES-BASED ORDER FOR LEO ACCESS, PROMOTING GLOBAL CONNECTIVITY ALIGNED WITH SDGs	EFFECTIVE IMPACT ONTO FURTHER DEVELOPMENT OF LEO RELEVANT POLICIES	RESOURCE-INTENSIVE: HUMAN RESOURCES, CAPACITY BUILDING, ACTIVE ENGAGEMENT	RECOMMENDED
OPTION 6	ENGAGED	"UNIVERSAL LEOs"	ACTIVELY ENGAGE IN EXISTING INTERNATIONAL AND REGIONAL FORUMS TO ENSURE POLICIES FACILITATE GLOBAL CONNECTIVITY AND SUSTAINABLE DEVELOPMENT GOALS.	EFFECTIVE IMPACT ONTO FURTHER DEVELOPMENT OF LEO RELATED POLITICIES	NONE	STRONGLY RECOMMENDED

Source: authors' own work.

Conclusions

Global satellite broadband networks have the potential to significantly enhance internet resiliency, complement mobile telecommunications, and extend connectivity benefits to underserved areas. As the digital divide persists across various regions, satellite broadband offers a promising solution to ensure more equitable Internet access. However, realising these benefits relies on several critical steps nations must undertake to ensure cybersecurity. It is a significant endeavour that requires proactive and effective domestic regulation, fostering awareness, building capacity, acquiring knowledge and expertise, and forming alliances. The persistence of cybersecurity concerns could hinder the effective deployment of satellite technology and its potential developmental benefits. Given the growing reliance on satellite broadband in global connectivity, it is imperative to find timely solutions to these challenges. Cybersecurity has been a contentious issue in multilateral

discussions, often leading to stalemates. Nonetheless, domestic regulators should remain vigilant in monitoring these developments, no matter how gradual, and should actively defend their interests—preferably in collaboration with others who share similar concerns. Additionally, they should follow the expert reports produced by independent organisations and regulatory initiatives addressing cyber vulnerabilities associated with space technologies.

The cybersecurity implications of the six prevailing domestic policy responses analysed above each carry their specific risks. However, a thorough understanding of each option will enable domestic regulators to implement appropriate cybersecurity measures. Independent of their policy choices, they should all conduct a thorough review of their domestic laws concerning the authorisation and licensing of LEOs to determine whether they are adequate to address their cybersecurity concerns. This review must respect considerations related to cybersecurity, ensuring that local laws and regulations adequately protect data security, critical infrastructure and users. Their assessment can significantly benefit from research and domestic regulatory interventions of spacefaring countries, which have more experience and expertise. Again, independent of the policy choice, advocating multilateral, if not regional, approaches to satellite broadband deployment and their cybersecurity can enhance the effectiveness of broader Internet infrastructure cybersecurity. If part of their policy, market efficiency can be achieved by encouraging collaboration among neighbouring states and optimising resource allocation. To effectively represent shared interests, existing regional organisations can help unite efforts among member states, enhancing collective knowledge and capacity. By collaborating within these frameworks, nations can align their regulatory practices and share best practices for satellite broadband deployment. This approach fosters a more cohesive strategy for addressing the challenges and opportunities presented by satellite technology. Harmonising regulatory policies across nations and international organisations is another essential step for facilitating the growth of satellite broadband networks. Regulatory agencies must work to align their national LEO policies and cybersecurity requirements with those of other nations and international bodies, creating comprehensive approaches to cybersecurity, telecommunications, and internet governance. Such alignment is particularly important as the complexity of global communications continues to evolve with the advent of new technologies.

Bibliography

ENISA, *Definition of Cybersecurity – Gaps and Overlaps in Standardisation*, Brussels 2015. Available at: https://www.enisa.europa.eu/sites/default/files/publications/Cybersecurity_Definition_Gaps_v1_0.pdf (accessed: 31/12/2024).

European Commission, EUSPA, *The Secure SATCOM Market and User Technology*, Brussels 2023.

European Commission, *The Future of European Competitiveness: Part B – In-depth Analysis and Recommendations*, Brussels 2024, p. 173 ff. Available at: https://commission.europa.eu/topics/eu-competitiveness/draghi-report_en/ (accessed: 31/12/2024).

European Union Agency for Cybersecurity (ENISA), *LEO Satcom Cybersecurity Assessment*, Brussels 2024. Available at: https://www.enisa.europa.eu/publications/low-earth-orbit-leo-satcom-cybersecurity-assessment (accessed: 31/12/2024).

Graham, E., Lawmakers Reintroduce Legislation to Bolster Satellite Cybersecurity, *NextGov*, 4 May 2023. Available at: https://www.nextgov.com/cybersecurity/2023/05/lawmakers-reintroduce-legislation-bolster-satellite-cybersecurity/385991/ (accessed: 31/12/2024).

Internet Society, *Perspectives on LEO Satellites*, Massachusetts 2022. Available at: https://www.internetsociety.org/resources/doc/2022/perspectives-on-leo-satellites/ (accessed: 31/12/2024).

Internet Society, *The Internet and Sustainable Development*, Virginia 2015. Available at: https://www.internetsociety.org/resources/doc/2015/the-internet-and-sustainable-development (accessed: 31/12/2024).

Manner, J., *Spectrum Wars: The Rise of 5G and Beyond*, Artech House, Virginia 2021.

OFCOM, *Wider regulatory obligations*, 30 January 2023. Available at: https://www.ofcom.org.uk/spectrum/space-and-satellites/wider-regulatory-obligations/ (accessed: 31/12/2024).

Raman, S., **Weigel, R.**, **Lee, T.**, The Internet of Space (IoS): A Future Backbone for the Internet of Things?, *IEEE Internet of Things*, 8 March 2016. Available at: https://iot.ieee.org/articles-publications/newsletter/march-2016/the-internet-of-space-ios-a-future-backbone-for-the-internet-of-things.html (accessed: 31/12/2024).

SpaceX, Starlink System Architecture for Internet, *Techplayon*, 12 January 2024. Available at: https://www.techplayon.com/starlink-system-architecture/ (accessed: 31/12/2024).

Starlink, Available at: https://www.starlink.com/business/direct-to-cell (accessed: 25/07/2025).

Swallow, E., **Visner, S.**, It's time to declare space systems as critical infrastructure, *Politico*, 2 April 2021. Available at: https://www.politico.com/news/2021/04/02/its-time-to-declare-space-systems-as-critical-infrastructure-478848 (accessed: 31/12/2024).

Voelsen, D., *Internet from Space*, Stiftung Wissenschaft und Politik Research Paper, 2021, 6. Available at: https://www.swp-berlin.org/en/publication/satellite-internet (accessed: 24/02/2025).

Waterman, S., Beyond GEO: Major Operators Have A Multi-Orbit Focus, *Viasatellite*, 12 March 2020. Available at: https://interactive.satellitetoday.com/beyond-geo-major-operators-have-a-multi-orbit-focus/ (accessed: 31/12/2024).

Weber, R.H., Regulatory Autonomy and Privacy Standards under the GATS, *Asian Journal of WTO & International Health Law & Policy*, 2012, 7, pp. 25–47.
World Summit on the Information Society, *Tunis Agenda for the Information Society*, WSIS-05/TUNIS/DOC/6(Rev. 1), 18 November 2005. Available at: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html (accessed: 25/07/2025).

SECTION III

https://doi.org/10.18778/8331-719-9.09

The Gradual Dependence on Starlink and Its Impact on the Digital Organization of Arctic Territories in Canada

Célestine R. Rabouam[1]

Introduction

Satellite-based telecommunications systems are socially and politically constructed objects. They are not only determined by a technical dimension but also by the geopolitical contexts in which they are conceived, developed and used. Even though communication satellites orbit in outer space, their design, operation and the services they provide are firmly rooted in terrestrial policies.[2] The development of these systems and their improvement over time are the result of political, economic, social, ideological, philosophical and ethical choices (or lack thereof). This is one of the main reasons why the rapid development and deployment of low-earth orbit (LEO) satellite constellations is now at the center of social, economic and, above all, geopolitical issues, as these systems also profoundly change the spaces and territories in which they are embedded.

With more than 4 million subscribers in 100 countries as of September 2024,[3] the Starlink satellite constellation is attracting significant attention, especially as the company is now fully involved in strategic sectors such as the digital development

1 Institut Français de Géopolitique, Universite Paris 8, Paris, France.

2 B. Warf, Geopolitics of the satellite industry, *Tijdschrift voor Economische en Sociale Geografie*, 2007, 98, pp. 385–397.

3 A. Alamalhodaei, Starlink hits 4 million subscribers, *TechCrunch*, 26 September 2024. Available at: https://techcrunch.com/2024/09/26/starlink-will-hit-4-million-subscribers-this-week-spacex-president-says/ (accessed: 29/09/2024).

of underserved areas, Internet governance, and space governance. While it currently represents only a small proportion of global Internet traffic, Starlink is seen as an important tool for providing internet services in rural and remote regions where the installation of terrestrial infrastructure is complex and costly.[4]

Satellite constellations such as Starlink offer considerable potential for remote regions with limited access to digital resources. In 2023, the International Telecommunication Union estimated that approximately one-third of the world's population, or 2.6 billion people, still lack Internet access.[5] However, these inequalities are not solely due to a lack of telecommunications infrastructure. While many people could technically benefit from these technologies, financial barriers often prevent them from doing so. This problem is particularly pronounced in areas that rely on satellite communications, as the high cost of these services makes them inaccessible to many users. In the Canadian Arctic, this reliance on satellites is particularly critical, as geophysical and geographical challenges such as thawing permafrost, polar climate, extremely low population density and a lack of road infrastructure make it difficult to develop traditional digital infrastructure like cable. Nunavut in the Eastern Canadian Arctic is a notable example because the entire population and all services are completely dependent on satellite technology.[6] This heavy reliance not only hinders the decentralized governance of the territory, but also exacerbates social inequalities and the digital divide, disproportionately affecting the Indigenous population[7]—particularly the Inuit, who make up nearly 86% of Nunavut's population.[8]

The technical limitations of satellite telecommunications systems, combined with the geographic, climatic and geophysical challenges associated with Canada's Arctic regions, have hampered their digital development. However, the organization and structure of the Arctic telecommunications market, which is dominated by the Internet service provider NorthwesTel, has also played an important role. NorthwesTel hardly cooperates with smaller competitors and invests mainly in the most populated and profitable areas, which exacerbates the inequalities between the Arctic communities. This situation has allowed constellations such as Starlink to quickly capture the market and position itself as a truly competitive player against NorthwesTel.

---

4 C. Rabouam, L'avènement des constellations de satellites dédiées au haut débit dans les territoires isolés: le cas de Starlink dans l'Arctique canadien, *L'Espace Politique*, 2024, 51–52(2023-3/2024-1), p. 2.

5 ITU press release. Available at: https://www.itu.int/fr/mediacentre/Pages/PR-2023-11-27-facts-and-figures-measuring-digital-development.aspx (accessed: 23/09/2024).

6 C. Rabouam, *op. cit.*, pp. 3–4.

7 M. Klyne, La Fracture Numérique Au Canada Pénalise Les Populations Autochtones et Rurales: Sénateur Klyne, *SenCa+*, 8 February 2023. Available at: https://sencanada.ca/fr/sencaplus/opinion/la-fracture-numerique-au-canada-penalise-les-populations-autochtones-et-rurales-senateur-klyne (accessed: 24/09/2024).

8 Statistique Canada, *Inuit: Fact Sheet for Nunavut*, 29 March 2016. Available at: https://www150.statcan.gc.ca/n1/pub/89-656-x/89-656-x2016017-eng.htm (accessed: 24/09/2024).

In Nunavut, and to a lesser extent in Yukon and the Northwest Territories, the reliance on satellites, the lack of competition and the resulting unstable and expensive services have created a particularly favorable environment for the rise of constellation operators such as Starlink and OneWeb.[9] In this context, anticipated improvements in the technical performance of satellite systems have been eagerly awaited, as the geographic and geophysical constraints in the Canadian Arctic make these technologies essential for an equitable connectivity solution across the territory. The launch of Starlink, which positions itself as both a competitive Internet provider and a partner for local stakeholders, has sparked great optimism in isolated communities of the Canadian Arctic. However, it also raises growing concerns about the potential hegemony of private American players over space telecoms infrastructures and network topology, which are fundamental spaces for the expression of economic and political power.[10]

The operational deployment of LEO satellite constellations in the Canadian Arctic is inherently a geographic and geopolitical issue. The deployment of this new telecommunications system in territories still dependent on satellites changes the spatial logic of infrastructure organization while redefining power dynamics between the actors traditionally involved in the digital development of these territories (federal government, territorial government, traditional service providers, Indigenous organizations). The technological evolution of satellites thus contributes to the redefinition of power relations at local, regional and global levels, as the development and control of these technologies is concentrated in the hands of a minority of state and private actors who can use them to strengthen their economic, military or cultural influence.[11]

By focusing on the case of the Canadian Arctic, this article aims to examine the different effects of the arrival of broadband satellite constellations on the digital organization of these territories. It also aims to show how Starlink's strategy of rapid adaptation to local actors, particularly in Nunavut, has enabled rapid integration into the territory's digital ecosystem and has even become a key element within it.

The first part of this article will aim to demonstrate that various factors are hampering the digital development of the Canadian Arctic regions. The second part will then examine the opportunities and challenges arising from the improvement of satellite communication systems and their increasing control by private actors. Finally, the third part will aim to identify the concrete impacts of the growing reliance on Starlink on the digital organization of the Canadian Arctic, with a particular focus on Nunavut.

9 C. Rabouam, *op. cit.*, pp. 31–36.

10 F. Musiani et al. *Governance by Infrastructure*, [in:] F. Musiani, D. Cogburn, L. DeNardis, N. Levinson (eds.), *The Turn to Infrastructure in Internet Governance. Information Technology and Global Governance*, Palgrave Macmillan, New York 2016, pp. 3–21.

11 C. Rabouam, *op. cit.*, p. 4.

The digital organization of arctic territories in Canada: unequal development shaped by various factors

The challenges in developing digital infrastructure in the Arctic territories

The territories that make up the Canadian Arctic (Yukon, Northwest Territories and Nunavut) are unequally connected to the rest of Canada from a physical standpoint. While Yukon and the Northwest Territories (NWT) have a road network, Nunavut is only accessible by air or sea. In terms of telecommunications, these three territories are not connected in the same way or with the same technologies. Telecommunications services in the Yukon rely almost exclusively on land-based fiber optic cable, with the exception of one satellite-dependent community, the NWT relies on a combination of technologies (satellite, cable and microwave tower networks), and Nunavut relies entirely on satellite-based telecommunications systems.[12]

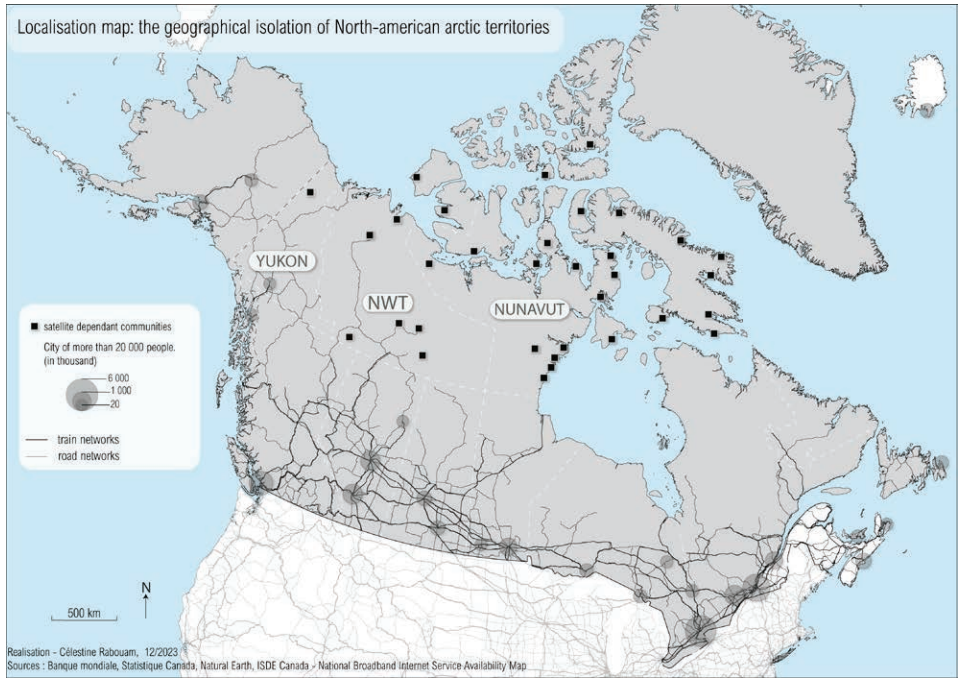


Fig. 1. Localisation map: geographical isolation of North American Arctic territories
Source: author's own work.

12 M. Delaunay, *Internet dans l'Arctique canadien, enjeu de Soft Power pour l'État fédéral et les Inuit*, Université de Paris-Saclay, Paris 2021, p. 221. Available at: https://theses.hal.science/tel-03599610/ (accessed: 24/09/2024).

Geostationary (GEO) satellites[13] are extremely practical communication systems for connecting the most remote and isolated communities, as they allow coverage of vast areas and avoid the constraints of building traditional digital infrastructures such as fiber optic cables. This is one of the main reasons why the Canadian federal government and Internet Service Providers (ISPs) have chosen to connect numerous rural and Arctic communities via this technology.

In the Canadian Arctic, the technical and economic challenges associated with laying cables or microwave tower networks indeed necessitate the use of satellites. The installation of terrestrial infrastructure is subject to extreme weather conditions and the instability of permafrost, while the laying of underwater cables in the Northwest Passage requires significant feasibility and environmental impact studies, as this maritime route is covered with ice for part of the year. If the cable is damaged by ice cracking or any other cause, the repair will be even more costly, as the contractors will have to wait to rent a vessel capable of navigating Arctic waters and wait until summer to repair the cable, which would be unusable until then. Furthermore, even if an underwater cable were to reach these Arctic waters, the costs associated with deploying the final kilometers of cable to connect communities and end users would be too high and would likely be passed on to the users.

Indeed, the demographic distribution and low population density of these areas pose a major challenge for large-scale infrastructure projects, and the most significant projects—such as the *Dempster Fiber Project* and the *Mackenzie Valley Fiber Link*—are generally concentrated in the more populated areas. The regional capitals of Yukon (Whitehorse) and the NWT (Yellowknife) are the two largest population centers in the Canadian Arctic and are being connected to fiber because their populations of 20,000 to 30,000 people make terrestrial infrastructure projects financially viable. In the least populated communities and even in Iqaluit, the capital of Nunavut, with a population of about 7,000 people, the profitability of a cable project is far less attractive.

In addition, the Arctic territories are particularly vast and there are very few road networks, along which wireless telecommunications infrastructure, microwave towers and fiber optic cables are usually installed. The most striking example is Nunavut: this territory, which covers more than 2 million square kilometers, has no roads connecting communities to each other or to the rest of Canada, and it is also the least well-connected territory on a national scale.[14] The polar climate and the presence of permafrost further complicate the logistical processes required to establish terrestrial infrastructure (feasibility studies, construction time, maintenance and durability of infrastructure, upgrades). In the Northwest Territories, the territorial government supported the installation of a fiber optic cable in the Mackenzie Valley back in 2014. This project connected several communities that relied

13 These satellites circulate in a geostationary orbit (circular or geosynchronous) at an altitude of approximately 36 000 km from the users.

14 C. Rabouam, *op. cit.*, p. 29.

on satellites. However, Ledcor, the company laying the cable, faced significant geological challenges caused by permafrost along the cable route.[15]

These geographic, demographic, and geophysical constraints have played an important role in the entrenchment of satellite dependence in Arctic communities, but this dependence has also been reinforced by the decisions of federal and territorial governments as well as local administrations. The financial and logistical investments of these stakeholders are essential to support the digital development of Arctic territories, and most telecommunications projects are therefore funded through federal or territorial government grants. In Nunavut, public investment support has proven essential since the launch of the first Internet services. The Qiniq network, which was rolled out to all Nunavut communities in 2005, was made possible primarily through $ 175 million in public and private investment, which helped maintain a minimum service rate of $ 80 per month until 2018.[16]

A market traditionally controlled by the Bell Canada—NorthwesTel—Telesat trio

The federal government's support for the Canadian satellite operator Telesat also played an important role in the decision to connect people in the Arctic via satellite technology. Telesat was founded in 1969 with public funding, and its first satellite, Anik A1, launched from Cape Canaveral in 1972, provided some Arctic communities with access to telephone services as early as January 1973.[17] In fact, the name of the first satellite "Anik"—which means "little brother" in Inuktitut—was intended to echo the Inuit population it would primarily serve in the north, at a time when Inuit claims in Canada were becoming increasingly important. The operator then received substantial government subsidies until its privatization and takeover by Bell Canada in 1998.[18] Bell Canada is also the parent company of NorthwesTel—the main Internet and telephone provider in the Canadian Arctic—and Bell Mobility, which provides cellular and Internet services in the Far North. In satellite-dependent communities, NorthwesTel and Bell Mobility rely on Telesat's satellite bandwidth. However, it is important to note that NorthwesTel had a stronger presence in Yukon and the Northwest Territories in the past. Initially, the company focused on the more populated communities in Nunavut and only expanded its services to all communities in Nunavut in 2019 with the help of a federal grant of approximately 50 million dollars.[19] Another Internet service provider, SSi Micro, was already present in satel-

15 D. Thurton, Inspection reports cite environmental concerns with Mackenzie Valley fibre optic project, *CBC News*, 1 February 2016. Available at: https://www.cbc.ca/news/canada/north/mackenzie-valley-fibre-inspection-1.3428012 (accessed: 29/09/2024).

16 M. Delaunay, *op. cit.*, p. 294.

17 R. Collins, *Une voix venue de loin. L'histoire des télécommunications au Canada*, McGraw-Hill Ryerson Limited, Toronto 1997, p. 263.

18 L. St. Germain, Fire, Ice, and Politics: The Evolution of Domestic Satellite Communications in Canada, *IEEE Conference on the History of Electronics*, 2004, p. 16.

19 Ottawa gives Northwestel $50 million to improve Nunavut internet, *Nunatsiaq News*, 15 September 2017. Available at: https://www.qiniq.com/wp-content/uploads/2017/10/NO-2017-09-15.pdf (accessed: 06/11/2024).

lite-dependent communities in the Northwest Territories, as well as in all Nunavut communities. SSi Micro also participated in connecting all Nunavut communities to the Internet for the first time using the Qiniq network in 2005.[20]

The subsidies granted by the government and federal authorities partly increase the dependence on satellites in the Arctic territories and at the same time prevent real competition in the telecommunications market. On the one hand, the subsidy programs will always pick one winner instead of distributing the money to several players; on the other hand, the subsidies are almost systematically awarded to NorthwesTel or SSi Micro, which already have know-how and infrastructure in the North. For the authorities that run these subsidy programs, such as the Canadian Radio-television and Telecommunications Commission (CRTC), projects to improve satellite-based telecommunications services also have the advantage of covering multiple communities or territories, unlike terrestrial infrastructure projects that usually only connect a few communities.

Government decisions—at both the federal and territorial levels—regarding the funding of telecommunications projects have thus also contributed to the continued reliance of many Arctic communities on satellite technology. These decisions also explain the slow and complex implementation of cable projects in these regions. This situation is particularly evident and problematic in Nunavut, where investment has focused so heavily on satellite technology and infrastructure that it has now become difficult to envision a financially viable basis for developing terrestrial infrastructure. Satellites are expensive, and public investment to support their deployment in Canada is extremely high. For example, between 2002 and 2014, more than $200 million of public money was spent to bring satellite connectivity to remote areas of Canada, and this estimate does not take into account the various funds that have been established to provide coverage to remote areas.[21]

A reliance on satellites that exacerbates inequalities in access to digital resources

Satellite communications are very costly, both for ISPs, who commit to expensive long-term contracts with satellite operators, and for users. Internet plans are particularly costly and offer very limited data. For example, NorthwesTel's largest plan includes only 300 GB of data per month for $109, which is especially restrictive for remote workers or families with multiple users.[22] Moreover, NorthwesTel customers often face very high overage fees when they exceed their data limit.[23]

---

20 M. Delaunay, *op. cit.*, p. 294.

21 Canadian Radio-television and Telecommunications Commission, *Rapport d'enquête sur les services par satellite*, Gouvernement du Canada, 2015, p. 55. Available at: https://crtc.gc.ca/fra/publications/reports/rp150409/rp150409.pdf (accessed: 31/10/2024).

22 NorthwesTel Internet plans. Available at: https://www.nwtel.ca/internet-plans (accessed: 01/10/2024).

23 Canadian Radio-television and Telecommunications Commission, *Telecom Notice of Consultation CRTC 2022-147*, Gouvernement du Canada, 2022, pp. 10–12. Available at: https://crtc.gc.ca/eng/archive/2022/2022-147.htm (accessed: 10/10/2024)

In the Northwest Territories and Yukon, most of the population is connected via terrestrial cable or microwave towers. In Nunavut, on the other hand, the satellites operated by Telesat and SES Networks (since 2020) are the only systems that provide bandwidth to the entire territory. This reliance on just two satellites leads to significant bandwidth congestion issues, despite improvements made on these geostationary satellites in terms of throughput. At peak times, the volume of data packets—which are converted into signals to reach the satellite and connect users to the Internet—is usually too large for the system to handle all user requests, resulting in higher latency.[24] In general, the latency of satellite communication is much higher than that of fiber optic communication. The time it takes for data to travel between the different equipment (satellites, ground stations and user terminals) results in very high latency, which widens the gap between users with fiber optic connections and those who depend on these satellites. In addition, the distance that the signals have to travel to reach the different devices makes them vulnerable to terrestrial and extra-atmospheric weather interference.[25]

In Canada, reliance on GEO satellites hinders equitable access to digital resources for rural and Arctic populations, not only because their cost excludes a portion of the population, but also because they no longer meet the needs of users today. However, this system will always be part of the connectivity solution in territories like Nunavut, as it will likely never be possible to install redundant cables or microwave towers in all communities due to geographic, geophysical and demographic constraints.

For many years, Inuit organizations and local authorities in Nunavut have been soliciting investment in cable projects, but these projects will only connect a few communities. One cable project is being undertaken by the Government of Nunavut to connect the capital city of Iqaluit, and two others are being led by private Inuit organizations and supported by regional Inuit associations. The Sednalink project, led by the Inuit company CanArctic Inuit Networks, also aims to connect the capital city of Iqaluit, and the *Kivallik Hydro Fiber Link* project will connect five communities in southern Nunavut.[26] These projects do not aim to connect all Nunavut communities to the fiber network, but rather to free up satellite bandwidth for the rest of the territory.

---

24 Propagation latency is the term to describe the time it takes to transmit from source to destination across a network.

25 C. Rabouam, *op. cit.*, p. 8.

26 Nukik Corporation, *Kivalliq Hydro-Fibre Link*. Available at: https://www.nukik.ca/kivalliq-hydro-fibre-link/ (accessed: 10/10/2024).

The Operational Launch of Satellite Constellations: Opportunities and Challenges for Local Stakeholders

Improved performance of communication satellites from GEO to LEO: A game-changing development for satellite-dependent communities

Geostationary satellites are indeed a very effective technology to circumvent the constraints of installing terrestrial infrastructure in Arctic regions. Positioned about 36,000 km from Earth, these systems allow for the connectivity of vast areas through large transmission and reception beams, but the latency caused by the distance between the satellite and terrestrial equipment poses several problems. These systems also raise numerous technical and financial challenges, both for users and for the Internet service providers that rely on them. On the one hand, the technological vulnerability of satellites and the lack of alternatives to ensure communications redundancy mean that Arctic networks are not very resilient, and on the other, the cost of satellite communications excludes part of the population from having access to them, leading to major inequalities in access to digital resources.

Improving the technical performance of satellite telecommunication systems is therefore essential to envision a more equitable and fair connectivity solution for all Arctic communities. By reducing the distance between ground equipment and satellites and increasing their number to cover the entire globe (or a large part of it), operators of low-earth-orbit satellite constellations aim precisely to enable the most remote areas to benefit from latency times closer to those of fiber optic networks. The Starlink and OneWeb constellations currently available in the Canadian Arctic have their satellite fleets positioned at altitudes between 500 and 2,000 km, which is a significant difference from geostationary satellites.

When a user connects to the Internet via a GEO satellite connection, their data packets are converted into signals by their user terminal before traveling through outer space to the satellite. The satellite then decodes the user's request and sends the signal to a ground station connected to an Internet backbone. The signal must then travel back to the satellite at an altitude of 36,000 km and then back down to the user terminal to connect it to the Internet. These round trips between the user terminal, the satellite and the ground station have a noticeable impact on latency times for users. In general, the propagation latency is not perceptible to the user, as the data packets converted into signals travel at the speed of light between network equipment.[27] The speed of light in a vacuum is 299,792 km/s,

27 C. Rabouam, *op. cit.*, pp. 8–10.

while it is estimated to be around 200,000 km/s in fiber optic cables.[28] Latency is generally lower in fiber optic communications than in satellite communications because the distances traveled by data at the speed of light are shorter. Even if the data is transmitted via a cable encircling the Earth (approx. 40,000 km), the distance—and therefore ultimately the theoretical latency time—is shorter than with satellite communication. With a geostationary satellite, the data must travel 36,000 km to the satellite and then back to earth (72,000 km). Furthermore, an additional round trip is usually required for the data to reach the gateway station of the Internet service provider, which is connected to an Internet backbone.[29]

Some constellation operators also rely on inter-satellite optical links, which allow data to travel from one satellite to another at the speed of light to quickly reach a ground station connected to an Internet backbone and then the user's terminal device. This system helps to reduce latency and the need for ground infrastructure by creating an interconnected mesh network. Users' data packets are routed from satellite to satellite until they reach the nearest ground station, then back to a satellite and onwards via the satellites in the constellation to the one closest to the user before reaching their terminal.[30] Currently, the second generation of Starlink satellites is the only one equipped with this technology. This allows the operator to avoid the costs of building ground stations in the Arctic to operate its system.[31]

The importance of public investments in satellite in Canada

Improving the capabilities of communications satellites is consistent with specific geopolitical contexts at different levels. In Canada, Justin Trudeau's Liberal government has been working for many years to implement a digital policy aimed at both bridging the digital divide and reducing reliance on American digital players and infrastructure. For example, in June 2024, a law backed by the Trudeau government came into effect that levies a 3% tax on foreign tech giants that generate revenue from Canadian users—a measure that is being contested by the US Government.[32]

In this context, the Canadian operator Telesat has been working on the development of its own high-speed satellite constellation since the project was announced in 2017. Telesat's Lightspeed constellation was one of the first to be announced,

28 S. Bigo and J-P Hamaide, La fibre optique embobine la Terre, *Pour la Science*, 2006. Available at: https://www.pourlascience.fr/sd/physique/la-fibre-optique-embobine-la-terre-2448.php (accessed: 25/10/2024).

29 C. Rabouam, *op. cit.*, pp. 8–10.

30 I. Rodríguez-Pérez et al. Inter-satellite links for satellite autonomous integrity monitoring, *Advances in Space Research*, 2011, 2(47), pp. 197–212.

31 J. Foust, SpaceX adds laser crosslinks to polar Starlink satellites, *SpaceNews*, 26 January 2021. Available at: https://spacenews.com/spacex-adds-laser-crosslinks-to-polar-starlink-satellites (accessed: 12/10/2024).

32 G. Malone, Les États-Unis s'opposent à la taxe canadienne sur les services numériques, *La Presse*, 2 July 2024. Available at: https://www.lapresse.ca/affaires/2024-07-02/les-etats-unis-s-opposent-a-la-taxe-canadienne-sur-les-services-numeriques.php (accessed: 15/10/2024).

after Oneweb and Starlink in 2015 and before Amazon's Kuiper project in 2019. Originally, the constellation was to be built in partnership with Thales Alenia Space and consist of around 300 satellites. However, problems in securing sufficient investment prompted Telesat to reduce the number of satellites to 198 and replace the prime contractor with the Canadian company MDA Space.[33] Telesat, which was experiencing severe financial difficulties,[34] eventually received support from the Canadian federal government and the Quebec government, which enabled the company to move forward with its Lightspeed constellation project. This support came in the form of two loans: The federal government provided CAD 2.14 billion with various interest – rate agreements, and the Quebec government provided CAD 400 million, with terms largely reflecting those of the federal loan.[35]

The constellation will thus consist of 198 satellites distributed across several orbits, providing complete global coverage, including the polar regions. Like Starlink, Lightspeed will use optical links between the satellites and aims to optimize the performance of the network as much as possible.

In the case of Lightspeed, the substantial financial involvement of the Canadian and Quebec governments can be seen as a clear effort to regain control of rural and Arctic telecommunications at the national level. Since 2015, the federal government has launched numerous programs to bridge the digital divide in Canada, but these efforts to connect rural areas to high-speed Internet remain insufficient. In a March 2023 report by the Auditor General of Canada pointed out that the gap between urban areas and other regions could lead to equity issues as jobs, education and many services are dependent on Internet access. While nearly 91% of Canadian households had high-speed Internet access in 2021, only 59.5% households in rural and remote regions had the same access, a figure that drops to 42.9% households on First Nations reserves.[36]

The main goal of the Lightspeed constellation, then, is to provide a tangible technological solution for Canada's least connected population. It also aims to

33 Telesat Press Release, *Telesat Contracts MDA as Prime Satellite Manufacturer for Its Advanced Telesat Lightspeed Low Earth Orbit Constellation*, 11 August 2023. Available at: https://www.telesat.com/press/press-releases/telesat-contracts-mda-as-prime-satellite-manufacturer-for-its-advanced-telesat-lightspeed-low-earth-orbit-constellation/ (accessed: 25/10/2024).

34 J. Rainbow, Telesat still bullish on Lightspeed despite funding uncertainty, *Space News*, 30 March 2023. Available at: https://spacenews.com/telesat-still-bullish-on-lightspeed-despite-funding-uncertainty/ (accessed: 25/10/2024).

35 Telesat Press Release, *Telesat Completes $2.54 Billion Funding Agreements for Telesat Lightspeed Satellite Constellation with Strong Government Backing*, 13 September 2024. Available at: https://www.telesat.com/press/press-releases/telesat-completes-2-54-billion-funding-agreements-for-telesat-lightspeed-satellite-constellation-with-strong-government-backing/ (accessed: 25/10/2024).

36 R. Raycraft, Canada falling behind on connecting rural areas to high-speed internet: report, *CBC News*, 27 March 2023. Available at: https://www.cbc.ca/news/politics/federal-government-internet-rural-1.6792060 (accessed: 25/10/2024).

strengthen Canada's digital sovereignty and prevent this market from being completely dominated by foreign companies such as Starlink or OneWeb. Currently, these two constellations are the only ones operating in rural and Arctic areas of Canada. OneWeb has been available through Canadian distribution partners since the summer of 2022, and Starlink expanded its services to Yukon, the Northwest Territories and Nunavut in November of the same year.[37] In August 2021, OneWeb signed a Memorandum of Understanding with NorthwesTel, which was looking to expand connectivity solutions in Yukon and the Northwest Territories as part of its "*Every Community*" project. NorthwesTel originally planned to use the Telesat constellation, but eventually turned to OneWeb due to delays in the deployment of the Lightspeed constellation. The Canadian constellation, which was originally scheduled to be operational by 2024, has been significantly delayed compared to OneWeb and Starlink and has now postponed its launch to 2026.[38]

The arrival of the Starlink and OneWeb constellations in the Arctic market long before the launch of the Canadian Lightspeed constellation has resulted in a significant loss of influence for the Canadian operator Telesat. As Starlink and OneWeb launched their services first, they were able to quickly win over a large share of users and strengthen their partnerships with local players, reducing Telesat's influence in this market.

The impact of growing dependence on Starlink on the digital organization of Arctic territories: the case of Nunavut

Starlink's business model and its rapid adaptation to local stakeholders: an advantage over its competitors

In the Canadian Arctic, the lack of competition, the criticized practices of ISPs and the costly, unstable services they provide have led to strong demand from users and created particularly fertile ground for operators of low-earth orbit satellite systems. User criticism of NorthwesTel's services in satellite-dependent communities has focused primarily on the high cost of Internet plans that do not deliver the promised speeds, as well as significant overage fees.[39] While the company offers unlimited data plans in more populated areas where it operates fiber optic cable, these options are not available in satellite-dependent communities.

37 C. Rabouam, *op. cit.*, p. 34.

38 P.B. De Selding, Telesat may trim Lightspeed constellation size to counteract inflation; estimated in-service date now – 2026, *Space Intel Report*, 2022. Available at: https://www.spaceintelreport.com/telesat-may-trim-lightspeed-constellation-size-to-counteract-inflation-estimated-in-service-date-now-2026/ (accessed: 27/10/2024).

39 CRTC, *op. cit.,* pp. 10–12.

In this context, improvements in satellite system capabilities have been eagerly anticipated, and user frustration with the wait for reliable and efficient services has contributed greatly to the positive perception of Starlink and SpaceX CEO Elon Musk. The business model SpaceX adopted for its Starlink constellation has allowed the company to quickly establish itself in the Arctic digital ecosystem and even become an integral part of it. By selling its Internet packages directly to users without intermediaries, Starlink positioned itself as a real competitor to traditional ISPs. Initially perceived as a disruptive actor in contrast to OneWeb and Lightspeed, which both work with traditional ISPs, the American company eventually adapted its strategy to become both an ISP and a reseller of bandwidth in the same market.

By subscribing to Starlink, users can now bypass traditional ISP constraints, such as NorthwesTel's requirement that customers purchase a landline phone service in order to use an Internet package. NorthwesTel's largest package offers just 300 GB of monthly data for $109 (with no overage fees), while Starlink offers a package with 1 terabyte (about 8,000 GB) of data for $140 per month. Users can also exceed this data limit without additional costs, though their connection will then have a lower priority on the Starlink network, so the speed will be slightly slower once the terabyte has been reached.

Starlink represents an unprecedented shift for residential users, but also for companies and public administrations, which have so far been confronted with high basic fees that made Internet access a real economic challenge. The rapid deployment and adaptation of Starlink in the Canadian Arctic appears to have caught NorthwesTel off guard, as the company has lost significant share of the market in favor of Starlink. Even before SpaceX's service was available in the Arctic, NorthwesTel asked the CRTC for assistance in responding to the competitive threat posed by Starlink. In 2021, the company specifically asked the regulator to change the process for filing tariffs for retail Internet services to better prepare for the arrival of the American constellation.[40]

The arrival of Starlink and Oneweb represents a major change for users of the Arctic network. On the one hand, Starlink, as a private American player, offers a business model that truly competes with traditional Internet providers. On the other hand, the satellite systems of OneWeb and Starlink bring a new source of bandwidth to the Arctic and support telecommunication services in these areas.

A significant reconfiguration of power relations among actors traditionally involved in the digital development of the territory

The telecommunications market in the Canadian Arctic is dominated by three historical players: the satellite operator Telesat, Bell Canada and its subsidiary Northwestel. The emergence of a player like SpaceX in November 2022 therefore generated

40 Northwestel tells CRTC it's in "urgent" need of ability to respond to Starlink's competitive threat, *CARTT.CA*, 10 December 2021. Available at: https://cartt.ca/northwestel-tells-crtc-its-in-urgent-need-of-ability-to-respond-to-starlinks-competitive-threat/ (accessed: 25/10/2024).

as much concern for these incumbents as it did opportunity for smaller competitors like SSi Micro, who are trying to maintain their position in this market.

SpaceX has quickly integrated into the Arctic market by further developing the services of its Starlink constellation and adapting them to the specific needs of local communities. Originally targeting residential users, Starlink services were later extended to businesses and public administrations. About a year after the launch of its services, in December 2023, the American company announced its collaboration with SSi Micro through a federal grant of around 27 million dollars. This grant will enable SSi Micro to improve services in 25 communities in Nunavut by installing Starlink terminals and utilising the constellation's bandwidth.[41] A few months earlier, SpaceX had also announced the signing of an agreement with Rogers Communications—one of Bell Canada's main competitors in southern Canada— that would allow the company to launch its next service, "*Starlink Direct to Cell*", in the cellular sector.[42]

For its part, NorthwesTel relies on OneWeb services for satellite-dependent communities in the Northwest Territories and Yukon, but the company has no low-earth orbit satellite coverage for Nunavut. Under an agreement between operator Galaxy Broadband and PanArctic[43] (the private arm of the Qikiqtani Inuit Association dedicated to telecommunications), all of OneWeb's bandwidth capacity has been reserved for this territory and therefore cannot be used by NorthwesTel. The Inuit associations in Nunavut are particularly committed to projects to improve communication services, and the Qikiqtani Inuit Association has also tried to adapt to the emergence of satellite constellations in the market by setting up its own service. This attempt to adapt led to the creation of Inuknet in 2023, the first Inuit-owned Internet service provider to emerge from the partnership between OneWeb and Galaxy Broadband.[44]

The growing dependence on Starlink and its strategic consequences

On June 11, 2024, Bell Canada announced its intention to sell NorthwesTel to a consortium of First Nations, Métis, and Inuit from the Canadian Arctic. Presented as a "monumental" step that would contribute to national efforts towards

41 D. Lochead, Northern firm gets up to nearly $27M to speed up Nunavut's internet, *Nunatsiaq News*, 21 December 2023. Available at: https://nunatsiaq.com/stories/article/northern-firm-gets-up-to-nearly-27m-to-speed-up-nunavuts-internet/ (accessed: 25/10/2024).

42 Rogers Press Release, *Rogers Signs Agreement With SpaceX to Bring Satellite-to-Phone Coverage to Canada*, 26 April 2023. Available at: https://about.rogers.com/news-ideas/rogers-signs-agreement-with-spacex-to-bring-satellite-to-phone-coverage-to-canada/ (accessed: 25/10/2024).

43 D. Lochead, New company plans for faster internet in Nunavut, *Nunatsiaq News*, 1 May 2023. Available at: https://nunatsiaq.com/stories/article/new-company-plans-for-faster-internet-in-nunavut/ (accessed: 26/10/2024).

44 P. Lipscombe, Inuit-owned telco InukNet launches in Nunavut, Canada, *Data Center Dynamics*, 28 April 2023. Available at: https://www.datacenterdynamics.com/en/news/inuit-owned-telco-inuknet-launches-in-nunavut-canada/ (accessed: 26/10/2024).

reconciliation with Indigenous populations in Canada,[45] this sale also highlights Bell Canada's desire to gradually withdraw from the Internet market in the Arctic, as Starlink continues to establish itself as a key player in the sector.

In Nunavut, the territory's entire telecommunications infrastructure depends on satellites, and Starlink services are now widely used by the population. This dependence on satellites has made Nunavut, its government and its businesses important customers for the Canadian operator Telesat. Telesat also plans to build its own constellation with the help of federal investment. Its main goal is to improve connectivity for rural and Arctic populations in Canada — an objective already largely fulfilled by Starlink and OneWeb since their deployment in the Arctic in 2022. The Territorial Government of Nunavut, which previously relied on the NorthwesTel network[46] and thus Telesat's GEO satellite bandwidth, has also contracted with SpaceX to build a ground station in Iqaluit (the capital of Nunavut) and transfer government services to the Starlink network. Following this investment, the Department of Community and Government Services did not need to renew its contract with Telesat for $2.796 million and with Northwestel for $3.543 million.[47]

Starlink's rapid capture of the Arctic market also increases technological dependence, not only on satellite technology, but also on American infrastructure and players. Improving the performance of the government network by installing Starlink ground stations in Nunavut is taking place while the territorial government's submarine fibre optic cable project to Iqaluit is gradually being sidelined. This project was originally intended to eliminate the territory's dependence on satellites, but the territorial government now views investing in a cable as far more complex and risky than investing in satellite infrastructure. On the one hand, the benefits of this cable would only be visible in a few years, while the installation of Starlink ground stations can be completed in a few months. On the other hand, building a submarine cable to Iqaluit would require a significant logistical effort to bury and reinforce the cable to prevent it from breaking when sea ice forms in Baffin Bay. Although the cable project was of interest before the arrival of Starlink, given the market share that the American operator has now captured, there are no longer enough users for the cable to at least break even at the end of its life. From the territorial government's point of view, it therefore makes more sense to invest

45 Sixty North Unity, Northwestel and Bell Canada announce transformative partnership to advance economic reconciliation, *CISION*, 11 June 2024. Available at: newswire.ca/news-releases/sixty-north-unity-northwestel-and-bell-canada-announce-transformative-partnership-to-advance-economic-reconciliation-818958051.html (accessed: 10/10/2024).

46 NorthwesTel was used as the main network by the Government of Nunavut, as the company had built a fiber optic network in Iqaluit to connect the ground station and users more quickly. To ensure redundancy of government networks, the SSi Micro network was used as a back-up.

47 Legislative Assembly of Nunavut, *Letter from MDJ to COW Chair Hickes-Winter 2024 Commitments Follow Up*, 22 May 2024. Available at: https://assembly.nu.ca/sites/default/files/2024-05/2024-05-22-Letter%20from%20MDJ%20to%20COW%20Chair%20Hickes-Winter%202024%20Committments%20Follow%20Up-eng.pdf (accessed: 25/10/2024).

in a more efficient satellite infrastructure, as this is more cost-effective and can be used in the most remote communities.[48]

Starlink's capture of a large share of the Arctic telecommunications market also reinforces the technological dependence of Arctic networks on US infrastructure and operators. Indeed, the Starlink constellation and ground stations are US infrastructure, and SpaceX, whose industries are located in the US, is subject to US legislation. Furthermore, decisions made on the Starlink network, such as data routing strategies, are entirely determined by SpaceX.[49]

While there are numerous cable projects in Nunavut that could tangibly improve the territory's digital resilience, public investment in satellite technology remains predominant. Whether at the territorial level with the agreement between the Government of Nunavut and SpaceX for Starlink services or at the national level with the significant investments made by the Canadian and Quebec governments in the Lightspeed Telesat constellation, satellite still seems to be the preferred choice, although numerous studies, consultations and research show that it is necessary to rely on different technologies to make telecommunications more reliable for the population and all services in these territories.

Conclusion

The economic model of the Starlink constellation gives SpaceX control over its end-to-end network and positions the company as an increasingly influential and indispensable player in discussions about Internet governance, its standards, the regulation of outer space and the resources (launchers and frequencies) needed to access it. The emergence of satellite constellations in rural telecommunications markets also underscores the intense competition between private players and highlights the competitive threat that Starlink poses in the satellite telecommunications sector. The aim of low-earth orbit satellite constellations is to bridge the global digital divide and universalize Internet access. However, it's important to emphasize that these constellations also serve governmental and private interests that are often far removed from the concerns of communities still dependent on limited and costly Internet services.

In Nunavut, the favorable position and the rapid adaptation of Starlink to the specific needs of local actors concretely reinforce the logic of technological dependence on satellite technology, as well as on American infrastructure and actors

48 Interview conducted in Iqaluit on 09/30/2023. On file with author.

49 Boomerang routing refers to the fact that a significant proportion of Canadian Internet traffic, even domestic traffic, is routed via the United States - a person in Canada accessing a Web site physically located in Canada will generally see their data routed via the United States. See: A. Clement, *Canadian Network Sovereignty – A Strategy for 21st Century National Infrastructure Building*, Centre for International Governance Innovation, 26 March 2018. Available at: https://www.cigionline.org/articles/canadian-network-sovereignty/ (accessed: 06/11/2024).

in the most isolated communities of the Arctic. However, the introduction of Starlink and OneWeb services also represents the beginning of a new era for users in the Canadian Arctic. They now have slightly more options in terms of Internet service providers and access to higher-performing networks at more affordable prices. Satellites will likely always be part of the connectivity solution in the Canadian Arctic, and the arrival of these new players thus brings technological solutions to address the challenges associated with the digital development of these territories.

Bibliography

Alamalhodaei, **A.**, Starlink hits 4 million subscribers, *TechCrunch*, 26 September 2024. Available at: https://techcrunch.com/2024/09/26/starlink-will-hit-4-million-subscribers-this-week-spacex-president-says/ (accessed: 29/09/2024).

Bigo, **S.**, **Hamaide**, **J.-P.**, La fibre optique embobine la Terre, *Pour la Science*, 2006. Available at: https://www.pourlascience.fr/sd/physique/la-fibre-optique-embobine-la-terre-2448.php (accessed: 25/10/2024).

Canadian Radio-television and Telecommunications Commission, *Rapport d'enquête sur les services par satellite*, Gouvernement du Canada, 2015, p. 55. Available at: https://crtc.gc.ca/fra/publications/reports/rp150409/rp150409.pdf (accessed: 31/10/2024).

Canadian Radio-television and Telecommunications Commission, *Telecom Notice of Consultation CRTC 2022-147*, Gouvernement du Canada, 2022, pp. 10–12. Available at: https://crtc.gc.ca/eng/archive/2022/2022-147.htm (accessed: 10/10/2024).

Clement, **A.**, *Canadian Network Sovereignty – A Strategy for 21st Century National Infrastructure Building*, Centre for International Governance Innovation, 26 March 2018. Available at: https://www.cigionline.org/articles/canadian-network-sovereignty/ (accessed: 06/11/2024).

Collins, R., *Une voix venue de loin. L'histoire des télécommunications au Canada*, McGraw-Hill Ryerson Limited, Toronto 1997.

De Selding, P.B., *Telesat may trim Lightspeed constellation size to counteract inflation; estimated in-service date now – 2026*, *Space Intel Report*, 2022.

Delaunay, M., *Internet dans l'Arctique canadien, enjeu de Soft Power pour l'État fédéral et les Inuit*, Université de Paris-Saclay, Paris 2021.

Foust, J., *SpaceX adds laser crosslinks to polar Starlink satellites*, *SpaceNews*, 26 January 2021.

ITU, *Press release*. Available at: https://www.itu.int/fr/mediacentre/Pages/PR-2023-11-27-facts-and-figures-measuring-digital-development.aspx (accessed: 06/11/2024).

Klyne, M., *La Fracture Numérique Au Canada Pénalise Les Populations Autochtones et Rurales : Sénateur Klyne*, *SenCa+*, 8 February 2023.

Legislative Assembly of Nunavut, *Letter from MDJ to COW Chair Hickes-Winter 2024 Commitments Follow Up*, 22 May 2024.

Lipscombe, P., *Inuit-owned telco InukNet launches in Nunavut, Canada*, *Data Center Dynamics*, 28 April 2023.

Lochead, D., New company plans for faster internet in Nunavut, *Nunatsiaq News*, 1 May 2023. Available at: https://nunatsiaq.com/stories/article/new-company-plans-for-faster-internet-in-nunavut/ (accessed: 26/10/2024).

Lochead, D., Northern firm gets up to nearly $27M to speed up Nunavut's internet, *Nunatsiaq News*, 21 December 2023. Available at: https://nunatsiaq.com/stories/article/northern-firm-gets-up-to-nearly-27m-to-speed-up-nunavuts-internet/ (accessed: 25/10/2024).

Malone, G., *Les États-Unis s'opposent à la taxe canadienne sur les services numériques*, *La Presse*, 2 July 2024.

Musiani, F. et al. *Governance by Infrastructure*, [in:] F. Musiani, D. Cogburn, L. DeNardis, N. Levinson (eds.), *The Turn to Infrastructure in Internet Governance. Information Technology and Global Governance*, Palgrave Macmillan, New York 2016, pp. 3–21.

Northwestel tells CRTC it's in "urgent" need of ability to respond to Starlink's competitive threat, *CARTT.CA*, 10 December 2021. Available at: https://cartt.ca/northwestel-tells-crtc-its-in-urgent-need-of-ability-to-respond-to-starlinks-competitive-threat/ (accessed: 25/10/2024).

Nukik Corporation, *Kivalliq Hydro-Fibre Link*. Available at: https://www.nukik.ca/kivalliq-hydro-fibre-link/ (accessed: 06/11/2024).

Nunatsiaq News, Ottawa gives Northwestel $50 million to improve Nunavut internet, *Nunatsiaq News*, 15 September 2017. Available at: https://www.qiniq.com/wp-content/uploads/2017/10/NO-2017-09-15.pdf (accessed: 06/11/2024).

Rabouam, C., L'avènement des constellations de satellites dédiées au haut débit dans les territoires isolés: le cas de Starlink dans l'Arctique canadien, *L'Espace Politique*, 2024, 51–52(2023-3/2024-1).

Rainbow, J., *Telesat still bullish on Lightspeed despite funding uncertainty*, *Space News*, 30 March 2023.

Raycraft, R., *Canada falling behind on connecting rural areas to high-speed internet: report*, *CBC News*, 27 March 2023.

Rodríguez-Pérez, I. et al. *Inter-satellite links for satellite autonomous integrity monitoring*, *Advances in Space Research*, 2011, 2(47), pp. 197–212.

Rogers Press Release, *Rogers Signs Agreement With SpaceX to Bring Satellite-to-Phone Coverage to Canada*, 26 April 2023. Available at: https://about.rogers.com/news-ideas/rogers-signs-agreement-with-spacex-to-bring-satellite-to-phone-coverage-to-canada/ (accessed: 25/10/2024).

Sixty North Unity, Northwestel and Bell Canada announce transformative partnership to advance economic reconciliation, *CISION*, 11 June 2024. Available at: https://www.newswire.ca/news-releases/sixty-north-unity-northwestel-and-bell-canada-announce-transforma-

tive-partnership-to-advance-economic-reconciliation-818958051.html (accessed: 25/10/2024).

St. Germain, L., *Fire, Ice, and Politics: The Evolution of Domestic Satellite Communications in Canada*, *IEEE Conference on the History of Electronics*, 2004, pp. 1–18.

Statistique Canada, *Inuit: Fact Sheet for Nunavut*, 29 March 2016. Available at: https://www150.statcan.gc.ca/n1/pub/89-656-x/89-656-x2016017-eng.htm (accessed: 25/10/2024).

Telesat Press Release, *Telesat Completes $2.54 Billion Funding Agreements for Telesat Lightspeed Satellite Constellation with Strong Government Backing*, 13 September 2024. Available at: https://www.telesat.com/press/press-releases/telesat-completes-2-54-billion-funding-agreements-for-telesat-lightspeed-satellite-constellation-with-strong-government-backing/ (accessed: 25/10/2024).

Telesat Press Release, *Telesat Contracts MDA as Prime Satellite Manufacturer for Its Advanced Telesat Lightspeed Low Earth Orbit Constellation*, 11 August 2023. Available at: https://www.telesat.com/press/press-releases/telesat-contracts-mda-as-prime-satellite-manufacturer-for-its-advanced-telesat-lightspeed-low-earth-orbit-constellation/ (accessed: 25/10/2024).

Thurton, D., Inspection reports cite environmental concerns with Mackenzie Valley fibre optic project, *CBC News*, 1 February 2016. Available at: https://www.cbc.ca/news/canada/north/mackenzie-valley-fibre-inspection-1.3428012 (accessed: 29/09/2024).

Warf, B., Geopolitics of the satellite industry, *Tijdschrift voor Economische en Sociale Geografie*, 2007, 98, pp. 385–397.

https://doi.org/10.18778/8331-719-9.10

The Role of LEO Satellites for the (Cyber)Security Policies of Authoritarian States: The Case of Iran

Monika Stachoń[1]

Introduction

In recent years, intensifying global geopolitical rivalries and rapid technological advancements have driven states to explore alternative ways to enhance their defense capabilities. As global tensions escalate, outer space has emerged as a critical domain for defense and security, particularly for authoritarian states like Iran, where satellite technology provides strategic advantages, including in defense (notably, cyber defense).[2]

Iran, as one of the countries involved in international space exploration efforts, has been pursuing an expansive space program for years, aligning with its broader security strategy. Since 1958, when Iran joined the United Nations Committee on the Peaceful Uses of Outer Space, up to its contemporary ambitions for autonomous satellite technology capabilities, the nation's determination to strengthen its position on the global stage is evident.

Tehran's pragmatic approach to international cooperation is highlighted by its signing—but not full ratification—of key space treaties, such as the 1967 Outer Space Treaty. This stance reflects Iran's interest in international cooperation while maintaining flexibility in shaping its policies. Such an approach presents both

1 University of Warsaw, Poland.

2 This research was funded in whole by National Science Centre, Poland [grant no. 2021/41/N/HS5/01522].

opportunities and challenges in the broader context of global security and oversight. Under constant international pressure and isolated from traditional global communication and technological structures, Iran has invested in its technologies for many years. This has raised concerns over the dual-use potential of these technologies, which could serve not only peaceful space exploration but also ballistic missile program development.

Recently, low Earth orbit (LEO) satellites have gained particular significance for the Iranian government. Their lower production and launch costs compared to geostationary satellites facilitate easier access to advanced telecommunications and observational infrastructure. The lower orbital altitudes of these satellites enable faster data transmission and more efficient regional coverage. In recent years, LEO satellites have become a cornerstone of Iran's (cyber)security strategy. These technologies are employed not only for environmental monitoring and scientific support but also for military, intelligence, and regime control purposes.

This article analyzes the evolution of Iran's space program, illustrating how LEO technologies integrate into the broader context of national security and international space law. Particular attention is given to Iran's strategy of leveraging space as a tool to build technological autonomy and safeguard the regime's interests on the global stage. Satellites play a pivotal role in the regime's efforts to protect sovereignty, develop intelligence capabilities, and enhance cyber defense mechanisms. By examining the technological and political implications of Iran's use of LEO satellites, the article explores how these assets contribute to the state's broader strategic goals in security and resilience, including cyber resilience. The discussion is framed within conceptual and problem-oriented areas, encompassing topics such as norms and principles of international law related to cyberspace, responsible state behavior, critical infrastructure, data governance, and cybersecurity.

Iran and International Space Law

Iran's interest in outer space dates back to 1958, when it joined 17 other countries to establish the Ad Hoc Committee on the Peaceful Uses of Outer Space under the United Nations.[3] Two years later, Iran became one of the 24 founding members of the successor organization, the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS), established by General Assembly Resolution 1472 (XIV).[4]

3 United Nations, *Committee on the Peaceful Uses of Outer Space: Membership Evolution*. Available at: https://www.unoosa.org/oosa/en/ourwork/copuos/members/evolution.html (accessed: 02/02/2025).

4 In 1959, the United Nations General Assembly established the Committee on the Peaceful Uses of Outer Space (COPUOS) as a permanent body, initially comprising 24 members, and affirmed its mandate in Resolution 1472 (XIV). Since then, COPUOS has served as the central hub for international cooperation in the peaceful exploration and use of outer space.

Iran has also signed 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) of 1967,[5] although it has never ratified this agreement.[6] A similar status applies to the *Convention on Registration of Objects Launched into Outer Space* (Registration Convention) of 1975.[7] This indicates that Iran has expressed initial political and moral commitment to the issues covered by these documents but has not assumed the full legal obligations arising from them. If a treaty is not ratified, it cannot be automatically implemented within a country's domestic legal system. Consequently, the state is not formally a party to the agreement and cannot invoke its provisions or be held accountable for violating them.

However, the state is obligated to avoid actions contrary to the treaty's purpose and objectives until it clearly defines its stance on ratification. Only two of the five UN treaties on the use of outer space have been ratified by the Iranian government: the *Agreement on the Rescue of Astronauts, the Return of Astronauts, and the Return of Objects Launched into Outer Space* (1968)[8] and the *Convention on International Liability for Damage Caused by Space Objects* (1972).[9] Conversely, Tehran has not signed the *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies* (1979).[10] The status of Iran's participation in these agreements is summarized in the table below.

It maintains close contacts with governmental and non-governmental organizations involved in space activities, facilitates the exchange of information on space-related activities, and assists in exploring measures to promote international cooperation in this field. United Nations, *Committee on the Peaceful Uses of Outer Space*. Available at: https://www.unoosa.org/oosa/en/ourwork/copuos/index.html (accessed: 02/02/2025).

5 United Nations, *Treaty 2222 (XXI) on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*. Available at: https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html (accessed: 02/02/2025).

6 *Ratifications*. Available at: https://www.jus.uio.no/english/services/library/treaties/01/1-11/activities-exploration.html (accessed: 02/02/2025).

7 United Nations, *Convention on Registration of Objects Launched into Outer Space, General Assembly resolution 3235 (XXIX)*. Available at: https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/registration-convention.html (accessed: 02/02/2025).

8 United Nations, *Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, General Assembly resolution 2345 (XXII)*. Available at: https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/rescueagreement.html (accessed: 02/02/2025).

9 United Nations, *Convention on International Liability for Damage Caused by Space Objects, General Assembly resolution 2777 (XXVI)*. Available at: https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/liability-convention.html (accessed: 02/02/2025).

10 United Nations, *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, General Assembly resolution 34/68*. Available at: https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/moon-agreement.html (accessed: 02/02/2025).

Tab. 1. Status of Iran's ratification of international space treaties and agreements

Name of the treaty	Acronym	Admission Date	Status
United Nations treaties			
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)	OST	1967	Signed
Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space	ARRA	1968	Ratified
Convention on International Liability for Damage Caused by Space Objects (Liability Convention)	LIAB	1972	Ratified
Convention on Registration of Objects Launched into Outer Space (Registration Convention)	REG	1975	Signed
Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (Moon Agreement)	MOON	1979	X
Other agreements			
Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and under Water	NTB	1963	Ratified
Agreement Relating to the International Telecommunications Satellite Organization (ITSO)	ITSO	1971	Ratified
Agreement on the Establishment of the INTERSPUTNIK International System and Organization of Space Communications	INTR	1971	X
Convention Relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite	BRS	1974	X
Convention for the Establishment of a European Space Agency (ESA)	ESA	1975	X
Agreement of the Arab Corporation for Space Communications (ARABSAT)	ARB	1976	X

Name of the treaty	Acronym	Admission Date	Status
Agreement on Cooperation in the Exploration and Use of Outer Space for Peaceful Purposes (INTERCOSMOS)	INTC	1976	X
Convention on the International Mobile Satellite Organization	IMSO	1976	Ratified
Convention Establishing the European Telecommunications Satellite Organization (EUTELSAT)	EUTL	1982	X
Convention for the Establishment of a European Organization for the Exploitation of Meteorological Satellites (EUMETSAT)	EUM	1983	X
International Telecommunication Constitution and Convention	ITU	1992	Ratified

Source: Table presenting the status of Iran's ratification of international agreements on space activities as of January 1, 2024, prepared by the author based on: Status and application of the five United Nations treaties on outer space, and way and means, including capacity-building, to promote their implementation, Committee on the Peaceful Uses of Outer Space Legal Subcommittee, Vienna, 15–26 April 2024, https://www.unoosa.org/res/oosadoc/data/documents/2024/aac_105c_22024crp/aac_105c_22024crp_3_0_html/AC105_C2_2024_CRP03E.pdf (accessed: 02/02/2025).

Origins of Iran's Space Program

In 2005, Iran became the forty-third country in the world to possess satellites in outer space. However, the Iranian government's efforts in this area began much earlier. During the late 1940s and early 1950s, the Organization for Planning and Budget of the Country (*Sazeman-e Barname va Budje-ye Keshvar*) was established to oversee the development and strategic planning of Iran's economic and social systems. In 1974, within this framework, the Office for Satellite Data Collection was created to utilize satellite data and remote sensing technologies for infrastructure projects. Following preliminary research and successful outcomes from satellite imagery, the office was renamed the Iranian Remote Sensing Center (ITC),[11] marking the establishment of the nation's first space agency.

11 *Iranian Space Organization (Sazeman-e Fazayi Iran),* Ministry of Communications and Information Technology. Available at: https://web.archive.org/web/20080607133426/http://www.ict.gov.ir/companies-ministry-space-fa.html (accessed: 02/02/2025).

Shortly thereafter, the Iranian Remote Sensing Center initiated the Satellite Utilization Plan, which aimed to directly receive, process, reproduce, and distribute satellite data. To achieve this, three remote sensing satellite image reception stations were purchased and installed in Mahdasht Karaj. Simultaneously, under the rule of Shah Mohammad Reza Pahlavi, Iran became a member of the International Telecommunications Satellite Organization (ITSO).[12]

These developments marked the initial use of satellite technologies for civilian purposes, such as television signal transmission and telecommunications.[13] Iran became the fourth country globally to directly receive and process satellite images. However, Tehran's ambitious plans for space exploration were halted following the 1979 Islamic Revolution.

It was not until the 1990s that Iran's space program was revitalized. On October 6, 1991, a law was passed establishing the Iranian Remote Sensing Center. Under this law, the center became part of the Ministry of Post, Telegraph, and Telephone (now the Ministry of Communications and Information Technology) as a state-owned enterprise. Its primary objective was to prepare and utilize information derived from remote sensing technologies for research on land resources, meteorology, and oceanography to support macro-sectoral and regional development planning in production, infrastructure, and service sectors. Additionally, the center was tasked with conducting scientific research in remote sensing technology, promoting education, and encouraging the adoption and development of these technologies.[14]

The Iranian Remote Sensing Center also assumed responsibility for coordinating and monitoring space policy at the national level, covering both government and non-government sectors. Its specific tasks included:

- Developing remote sensing technologies to support the country's development and transformation;
- Minimizing dependence on foreign technology providers;
- Coordinating and supervising remote sensing activities conducted by other institutions, whether governmental, government-affiliated, or non-governmental, and proposing legislation and strategic documents in the field;
- Directly acquiring, processing, purchasing, producing, reproducing, selling, and distributing remote sensing data (including satellite and aerial imagery);
- Conducting research and studies to keep pace with technological advancements and promoting education and awareness in remote sensing technologies;
- Implementing joint projects with other domestic and international entities;

12 United Nations, *Agreement relating to the International Telecommunications Satellite Organization 'INTELSAT' (with annexes)*. Available at: https://treaties.un.org/Pages/showDetails.aspx?objid=08000002800e8e08&clang=_en (accessed: 02/02/2025).

13 *Iranian Space Agency*. Available at: https://www.undrr.org/organization/iranian-space-agency (accessed: 02/02/2025).

14 The Act on the Establishment of the Iranian Remote Sensing Center, 6 October 1991 (14 Mehr 1370 SH). Available at: https://rc.majlis.ir/fa/law/show/91955 (accessed: 02/02/2025).

- Establishing a national archive focused on maintaining, classifying, and updating remote sensing information;
- Researching the design, construction, and provision of equipment for acquiring, processing, interpreting, producing, and reproducing remote sensing information.[15]

The 1990s also witnessed intensified international cooperation in utilizing technologies to advance Iran's space program. In 1998, reports emerged of agreements with Russia and China for the design, construction, and launch of satellites. Notably, the Russo-Iranian agreement on technology transfer enabled Iran to develop its own research satellite named *Mesbah* ("Dawn," "Beacon," or "Lantern"). Although the purpose of *Mesbah* remains unclear, initial reports from 1999 described it as either a spy satellite, a communication satellite, or one intended solely for educational purposes.[16] The launch of *Mesbah* was planned for late 2005 aboard a Kosmos-3M rocket from the Plesetsk Cosmodrome, but the satellite was never sent into space.[17]

The structured development of Iran's space program gained momentum after 2004, when two key institutions were established: the Iranian Space Agency (ISA) and the Supreme Space Council (SSC). In addition, the Islamic Revolutionary Guard Corps (IRGC) operates its own space program. The roles and responsibilities of these entities will be described in the next section of the article.

Key Entities in Iran's Space Program

Supreme Space Council (SSC)

The Supreme Space Council was established under Articles 8 and 9 of Islamic Council Resolution No. 68159, dated December 13, 2003 (22 Azar 1382 SH). Its secretary is the head of the Iranian Space Agency (ISA). Although not an organization in itself, it functions as an auxiliary body at the ministerial level. Its members include:

- The President of the Islamic Republic of Iran, acting as the SSC's chairperson,
- Minister of Communications and Information Technology,
- Minister of Science, Research, and Technology,
- Minister of Defense,
- Minister of Foreign Affairs,
- Minister of Industry and Mining,
- Minister of Roads and Transportation,
- Director of Iran Broadcasting.[18]

15 *Ibidem*.

16 Y.S. Shapir, Iran's efforts to conquer space, *The Institute for National Security Studies Strategic Assessment*, 2005, 8(3), p. 8.

17 Mesbah 1, *Gunter's Space Page*. Available at: https://space.skyrocket.de/doc_sdat/mesbah-1.htm (accessed: 02/02/2025).

18 P. Tarikhi, Statutes of the Iranian Space Agency, *Journal of Space Law*, 2008, 34(2), pp. 3–7.

In 2007, the Supreme Administrative Council passed a resolution to consolidate all supreme councils in the country as part of the objectives of the Fourth National Development Plan. Consequently, the Supreme Council for Education, Research, and Technology (SCERT) was created but operated for only a few months. In February 2008, it was dissolved, and its responsibilities were transferred to the newly formed Science, Research, and Technology Commission (SRTC) under the government. However, on September 27, 2008, the Iranian Parliament (*Majles*) deemed the dissolution of 12 supreme councils unconstitutional and reinstated their operations, allowing the SSC to resume its activities.[19]

The SSC's primary objectives include formulating policies for the application of space technologies for peaceful purposes, overseeing the production, launch, and utilization of domestic research satellites, approving state-level and public sector programs related to space activities, encouraging private sector and cooperative partnerships in the effective use of space, and establishing guidelines for regional and international cooperation in space-related matters.[20]

Iranian Space Agency (ISA)

The Iranian Space Agency was established concurrently with the SSC under Articles 8 and 9 of Islamic Council Resolution No. 68159, dated December 10, 2003 (19 Azar 1382 SH),[21] and began its operations on February 1, 2004. According to its statute, adopted in 2008, ISA operates under the SSC's guidance and has a mandate to conduct all activities related to the peaceful utilization of space technologies. It engages in research, analysis, project management, engineering services, and space-related operations, including the application of remote sensing technologies.[22]

As an independent legal entity, the ISA is financially autonomous and affiliated with the Ministry of Communications and Information Technology.[23] It supports the ministry's Department of Satellite Communications Design, Engineering, and Installation and the Department of Satellite Communications Maintenance. It also collaborates closely with the Iranian Telecommunications Company.[24]

The agency's president, who also serves as the Deputy Minister of Communications and Information Technology and Secretary of the SSC, is appointed by the

19 *Ibidem*.

20 B. Harvey, H.H.F. Smid, T. Pirard, *Emerging Space Powers. The New Space Programs of Asia, the Middle East, and South America*, Chichester 2010, pp. 265–266.

21 Iranian Space Agency, *History of Iranian Space Agency*, 21 August 2019 (30 Mordad 1398 SH). Available at: https://web.archive.org/web/20210730123140/https://isa.ir/fa/general_content/41505-%D8%AA%D8%A7%D8%B1%DB%8C%D8%AE%DA%86%D9%87.html (accessed: 02/02/2025).

22 Article 1 of the Statute of the Iranian Space Agency, 13 June 2008 (24 Khordad 1387 SH). Available at: https://rc.majlis.ir/fa/law/show/134694 (accessed: 02/02/2025) (hereinafter referred to as the ISA Statute).

23 Article 2 of the ISA Statute.

24 Article 1 of the ISA Statute.

Minister of Communications and Information Technology.[25] The president is responsible for ensuring proper implementation of ISA's initiatives, safeguarding its rights and assets, managing the agency, and executing SSC-approved plans.[26]

The ISA's statute outlines 14 primary responsibilities, including:

- Developing and implementing medium- and long-term programs for the national space sector, in collaboration with related institutions, for submission to the SSC;
- Conducting research to shape policies for designing, producing, launching, and utilizing research and operational satellites, as well as delivering space services;
- Preparing plans for the peaceful use and development of space and space technologies;
- Strengthening national, regional, and international communication networks and monitoring their implementation in line with SSC policies;
- Conducting specialized studies, research, and education to advance space science and technology;
- Issuing permits and licenses for activities in space to ensure sustainable and coordinated use of space technologies and facilities, including satellites, direct reception stations, and satellite control centers.[27]

ISA also represents Iran in international and regional associations and unions related to space matters, advocating national interests in alignment with the regime's policies. It implements regional and international cooperative programs in space activities and maintains a national archive for centralizing, classifying, and updating space-related data.[28] All ISA activities must receive SSC approval, and its funding is derived from public budgets and allocated credits based on annual budgetary plans.[29]

Iranian Space Research Center (ISRC)

The Iranian Space Research Center (ISRC) was established in 2010 (1389 SH) with authorization from the Supreme Council for the Development of Higher Education to address the country's scientific and technological needs in space development. On January 28, 2015 (8 Bahman 1393 SH), the center was integrated into the Ministry of Communications and Information Technology. Alongside ISA, ISRC is one of the two primary organizations conducting space research and operations in Iran.[30]

25 Article 6 of the ISA Statute.
26 Article 7 of the ISA Statute.
27 Article 3 of the ISA Statute.
28 *Ibidem*.
29 Article 4 of the ISA Statute.
30 Iranian Space Research Center, *About*. Available at: https://web.archive.org/web/20220201170828/https://www.isrc.ac.ir/%D8%AF%D8%B1%D8%A8%D8%A7%D8%B1%D9%87-%D9%BE%DA%98%D9%87%D8%B4%DA%AF%D8%A7%D9%87 (accessed: 02/02/2025).

The ISRC's mission is to advance indigenous technologies, infrastructure, and systems for the peaceful utilization of space, enhancing human life in accordance with national priorities for sustainable scientific, technological, cultural, and economic development. It is a knowledge-based organization focused on innovative products in the realm of peaceful space technologies.

The center's three main objectives are:

- Conducting research to develop methods and techniques required by the Ministry of Industry, Communications, and Technology, aligned with the national space sector's vision;
- Creating infrastructure to promote education, research, and technological development in the space sector;
- Applying research achievements and space technologies to strengthen the space industry through commercialization or technology transfer and absorption in the private sector.[31]

To achieve these objectives, the ISRC is tasked with identifying research needs and developing plans to address the complete lifecycle of space technologies, conducting fundamental, applied, and developmental research on space telecommunications and remote sensing systems, and developing laboratory services and infrastructure for space-related activities. It also can run projects on advancing and refining operational software for space systems, collaborating with universities, research institutions, and both government and private scientific-industrial centers domestically and internationally, and promoting education and public awareness regarding the applications and achievements of domestic space technologies.[32]

The ISRC also operates five sectoral research institutes, focusing on satellite systems, propulsion systems, materials, energy, and mechanical research, distributed across Tehran, Tabriz, Isfahan, and Shiraz. In 2011 (1390 SH), the ISRC established the Space Systems Testing and Integration Center, supported by ISA, to aid in space product development and provide testing services to other industrial sectors, including aerospace, maritime, aviation, automotive, and telecommunications.[33]

Islamic Revolutionary Guard Corps (IRGC)

The Islamic Revolutionary Guard Corps (IRGC), established by Ayatollah Khomeini in May 1979, is one of the two components of Iran's armed forces alongside the regular military (*Artesh*).[34] Its constitutional mandate (Article 150) is to safeguard the Islamic Revolution and its achievements.[35] Unlike the military,

31 *Ibidem*.

32 *Ibidem*.

33 *Ibidem*.

34 K.M. Andrusiewicz, Korpus Strażników Rewolucji w systemie politycznym i polityce bezpieczeństwa Islamskiej Republiki Iranu, *Rocznik Bezpieczeństwa Wewnętrznego*, 2012/2013, pp. 361–362.

35 Islamic State of Iran, *The Constitution of the Islamic State of Iran*, Article 150 (*Qanun-e Asasi-ye Jomhuri-ye Eslami-ye Iran*). Available at: https://rc.majlis.ir/fa/law/show/132239 (accessed: 02/02/2025).

which adheres to a principle of non-interference in domestic affairs, the IRGC is a highly politicized institution with wide-ranging social, political, and economic influence.[36]

The IRGC's stated mission is "to protect the Islamic Revolution of Iran and its achievements, to persistently strive toward achieving divine goals, to promote the rule of divine law in accordance with the laws of the Islamic Republic of Iran, and to strengthen the foundations of the Islamic Republic through cooperation with other armed forces, military training, and organizing popular forces."[37] Unlike the regular Army, which adheres to a policy of non-interference in internal state affairs, the IRGC is a highly politicized institution due to its broad competencies.

Established shortly after the victory of the 1978–1979 Islamic Revolution, the IRGC was initially intended to serve as an ideological guard for the nascent regime. However, over the four decades of the Islamic Republic's existence, the IRGC's role has significantly evolved, far exceeding its original mandate. Today, in addition to performing typical counterintelligence duties, the IRGC functions as an expansive socio-political and economic conglomerate with influence in nearly every aspect of Iran's political and social life.[38] In practice, IRGC members represent a privileged and highly active group within Iranian society.

In addition to its political influence, the IRGC also plays a substantial role in the economy, encompassing nearly every sector of the Iranian market. Its economic involvement traces back to the Iran-Iraq War, during which the IRGC took control of confiscated factories and established the *Khatam al-Anbia* organization. This entity developed various companies operating in agriculture, industry, mining, transportation, road construction, import/export, and later education and culture. Over time, *Khatam al-Anbia* has become one of Iran's largest industrial and development contractors and is now regarded as the IRGC's primary engineering arm, undertaking contracts for constructing dams, water diversion systems, highways, water supply systems, and oil and gas pipelines.[39] Additionally, IRGC units are involved in the production of biological and chemical weapons and operate effectively in the oil, energy, and gas sectors. Their extensive network includes ties to various Iranian banks, further solidifying their pervasive role in the nation's economy.[40]

---

36 Islamic State of Iran, *The Constitution of the Islamic Revolutionary Guard Corps* (Asasname-ye Sepah-e Pasdaran-e Enghelab-e Eslami), dated September 6, 1982 (15 Shahrivar 1361). Available at: https://rc.majlis.ir/fa/law/show/90595 (accessed: 02/02/2025) (hereinafter referred to as the IRGC Constitution).

37 Article 1 of the Iranian Constitution.

38 F. Wehrey, J.D. Green, B. Nichiporuk, A. Nader, L. Hansell, R. Nafisi, S.R. Bohandy, *The rise of the Pasdaran, Assessing the Domestic Roles of Iran's Islamic Revolutionary Guards Corps,* RAND Corporation 2009. Available at: https://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG821.pdf (accessed: 02/02/2025), p. XI–XVIII.

39 *Ibidem*.

40 K.M. Andrusiewicz, *op. cit*., pp. 366–369.

The Islamic Revolutionary Guard Corps (IRGC) operates its own space program, likely initiated in the mid-to-late 21st century, which functions independently of Iran's civilian space program. Due to the IRGC's unique role and position within the state structure, it is not subject to oversight by the Supreme Space Council. This program was founded by Hassan Tehrani Moghaddam, often referred to as the father of Iran's missile program, and has primarily served as a cover for the development of long-range missile technologies.[41]

The unit responsible for developing and managing the IRGC's space program, including its ballistic missile initiatives, is the Islamic Revolutionary Guard Corps Aerospace Force (IRGC-ASF). According to the U.S. Defense Intelligence Agency (DIA), the IRGC-ASF oversees Iran's air defense operations in collaboration with the regular Iranian Army and serves as the primary operator of Iran's fleet of unmanned aerial vehicles (UAVs). Media reports and intelligence assessments indicate that the IRGC-ASF supervises the IRGC's space program and successfully launched its first military satellite, Noor-1, into orbit in April 2020.[42]

The IRGC-ASF operates through two key entities: IRGC Aerospace Force Self-Sufficiency Jihad Organization and IRGC Aerospace Force al-Ghadir Missile Command. The first one, established in 1993, is an Iranian research and development unit, which has been involved in ballistic missile research, flight testing, and the development and production of radar systems such as the Qadir.[43] The second one was listed by the European Union in 2010 as an entity associated with Iran's nuclear activities, particularly those related to the development of nuclear weapon delivery systems. This unit is likely directly responsible for managing Iran's ballistic missile operations.[44]

Aerospace Research Institute (ARI)

The Aerospace Research Institute (ARI) is a scientific and academic organization affiliated with the Ministry of Technology. Established in 2000, it has been actively engaged in conducting aeronautical research at the national level. The primary objective of the Institute is to identify and conduct research on advanced

41 J. Krzyzaniak, *Part 1: Explainer—Iran's Space Program*, *The Iran Primer*, United States Institute of Peace, 9 August 2022. Available at: https://iranprimer.usip.org/blog/2022/jun/03/explainer-irans-space-program (accessed: 02/02/2025).

42 Islamic Revolutionary Guard Corps (IRGC) Aerospace Force, *Iran Watch*, Wisconsin Project on Nuclear Arms Control, 24 August 2020. Available at: https://www.iranwatch.org/iranian-entities/islamic-revolutionary-guard-corps-irgc-aerospace-force (accessed: 02/02/2025).

43 Islamic Revolutionary Guard Corps (IRGC) Aerospace Force Self-Sufficiency Jihad Organization, *Iran Watch*, Wisconsin Project on Nuclear Arms Control, 24 February 2023, https://www.iranwatch.org/iranian-entities/islamic-revolutionary-guard-corps-irgc-aerospace-force-self-sufficiency-jihad-organization (accessed: 02/02/2025).

44 *IRGC-Air Force Al-Ghadir Missile Command*, Iran Watch, Wisconsin Project on Nuclear Arms Control, 2 March 2011. Available at: https://www.iranwatch.org/iranian-entities/irgc-air-force-al-ghadir-missile-command (accessed: 02/02/2025).

aeronautical and related technologies. ARI collaborates with private sector organizations to carry out innovative research in this field.

The Institute comprises three main departments: Aeronautical Sciences and Technologies, Space Sciences and Technologies, Law, Standards, and Management in the Aerospace Industry. ARI also oversees a Research Group on Aviation Physiology and a Think Tank focused on conducting strategic research in aerospace and planning for the future.[45]

ARI's core activities include designing and testing aerodynamic launch vehicles. It also has a dedicated group conducting research on suborbital rockets and their payloads. Additionally, ARI undertakes projects related to propulsion fundamentals and the performance of microsatellite propulsion systems, satellite software, public-private partnerships in space research, and the commercialization of space technologies. The Institute conducts and implements research projects in collaboration with the industrial sector, including the aviation industry, as well as the defense sector.[46]

Low Earth Orbit Satellites in Iran's Space Program

In 2005, Iran launched its first satellite into low Earth orbit (LEO). The *Sina-1* satellite was placed in space using a Russian Kosmos-3M rocket and was primarily intended for imaging and scientific research purposes. Subsequently, Iran achieved a significant milestone in 2009 by launching its first domestically manufactured satellite, *Omid*, using an indigenous launch vehicle, *Safir*. Table 2 provides an overview of low Earth orbit satellites launched by Iran since 2005, detailing the satellite name, year of launch, the launch vehicle used, and the satellite's primary application.

Tab. 2. A list of all Iranian low Earth orbit satellites, along with their launch vehicles and primary applications

LEO satellite	Launch vehicle	Main application
Sina-1 (2005)	Kosmos-3M (RU)	imaging and scientific research purposes
Mesbah (2005)	Kosmos-3M (RU)	environmental monitoring, data relay, and scientific experiments
Omid (2009)	Safir-1	data-processing, a store-and-forward communication mission
Rasad-1 (2011)	Safir-1B	imaging and reconnaissance, primarily environmental and topographical mapping

45 B. Harvey, H.H.F. Smid, T. Pirard, *op. cit.*, p. 268.
46 *Ibidem*.

Tab. 2 (cont.)

LEO satellite	Launch vehicle	Main application
Navid (2012)	Safir-1B	imaging and scientific research, primarily: atmospheric and weather studies, environmental monitoring, disaster management, and agricultural applications
Fajr (2015)	Safir-1B	remote sensing satellite, primarily: to capture high--resolution images for environmental monitoring, disaster management, and mapping.
Payam (2019)	Simorgh	environmental and agricultural monitoring, as well as for scientific and research purposes
Dousti (2019)	Safir-1B	remote sensing, with a focus on agricultural and geological data collection
Zafar 1 (2020)	Simorgh	monitoring natural disasters, forestry, and agricultural activities
Noor 1 (2020)	Qased	military satellite, for reconnaissance and surveillance purposes
Noor 2 (2022)	Qased	military satellite, for reconnaissance and surveillance purposes
Khayam (2022)	Soyuz (RU)	environmental monitoring, agricultural planning, and natural disaster management
Noor 3 (2023)	Qased	military satellite, for reconnaissance and surveillance purposes
Soraya (2024)	Qaem-100	research purposes
Mahda (2024)	Simorgh	test advanced satellite subsystems and monitor the performance of the multi-satellite release system
Keyhan-2 (2024)	Simorgh	improving the accuracy and functionality of Iran's satellite operations
Hatef-1 (2024)	Simorgh	enhancing Iran's communication capabilities
Pars-1 (2024)	Soyuz (RU)	environmental monitoring, including agricultural and geological studies

Source: prepared by the author based on media reports.

Over nearly two decades, the development of Iranian satellites highlights a clear shift in priorities and strategic goals. During the initial phase (2005–2012), missions predominantly focused on scientific research, environmental monitoring, and remote sensing (*Sina-1*, *Mesbah*, *Navid*). In this period, Iran primarily relied on Russian launch vehicles (Kosmos-3M), reflecting limited domestic capabilities in space technology.

Subsequently, a transitional phase (2015–2019) emerged, characterized by the deployment of more technologically advanced satellites, such as *Fajr*, which were

capable of capturing high-resolution imagery critical for crisis management and mapping. This phase also marked a period of intensive development of indigenous launch vehicles (*Safir-1B*, *Simorgh*).

Since 2019, there has been a significant acceleration in Iran's low Earth orbit (LEO) satellite program, demonstrated by numerous satellite launches serving a variety of purposes. These include environmental imaging (*Khayam*, *Pars-1*), military applications (*Noor-1*, *Noor-2*, *Noor-3*), and technological testing (*Mahda*, *Keyhan-2*). This period clearly indicates that Iran is currently in an expansion phase, with the development of launch systems such as *Qased* and *Qaem-100* underscoring Iran's growing autonomy in space exploration.

Iran's LEO satellite program plays a significant role in advancing the country's strategic technological capabilities, integrating civilian, scientific, and military objectives. A comprehensive analysis of this program necessitates understanding how individual LEO satellites are utilized. By classifying these satellites, one can discern Iran's technological priorities and strategic directions shaping the development.

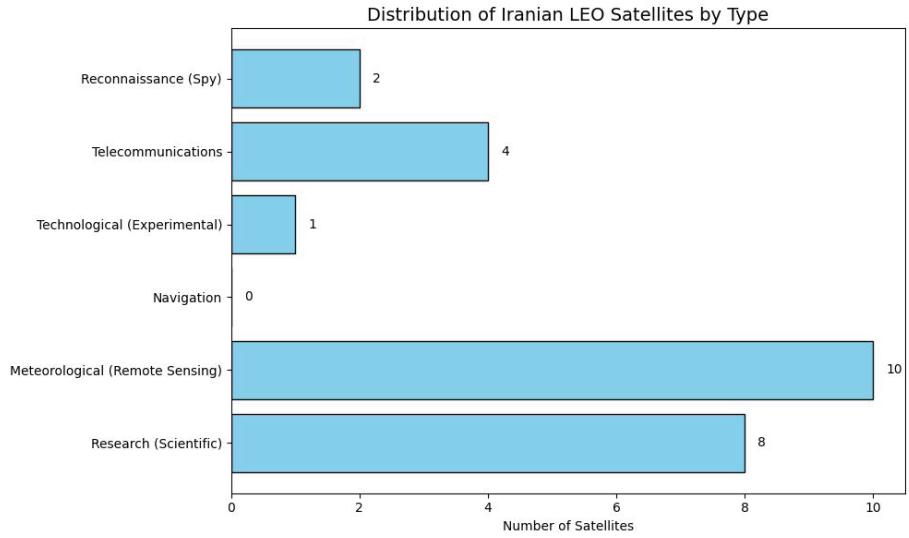


Fig. 1. A chart illustrating the distribution of purposes for which LEO satellites are utilized by Iran
Source: prepared by the author.

An analysis of Iranian low Earth orbit (LEO) satellites launched between 2005 and 2024 reveals five main categories of applications, differentiated by the number of units launched and their functions.

The most numerous category comprises meteorological and remote sensing satellites, accounting for a total of nine units. These satellites are critical for monitoring climate change, analyzing natural resources, and supporting crisis management, including disaster response. It can be inferred that Iran, as a nation vulnerable to

the effects of climate change and grappling with water scarcity, is investing in space technologies to facilitate sustainable resource management. Examples of such satellites include *Payam* and *Pars-1*, which are utilized for environmental monitoring, agricultural management, and geological resource mapping.

The second-largest group, comprising eight units, highlights the importance of Iran's space program for scientific research. These satellites are used for atmospheric observations, geodetic studies, and biological and astronomical experiments. The launch of units such as *Navid* and *Khayam* underscores Iran's aspirations to advance its scientific capabilities and technological innovation, which could enhance the country's prestige within the international scientific community.

In summary, during the initial phase of Iran's space program (2005–2012), the focus was predominantly on scientific research, environmental monitoring, and remote sensing. Since 2019, there has been a clear diversification in satellite applications, encompassing both civilian and military objectives. This period marks a significant acceleration in space-related activities, indicating Iran's growing technological capabilities and recognition of the strategic role its space program plays in national security.

Iran is gradually developing autonomous capabilities in satellite design and launch, reducing its dependence on countries like Russia. Simultaneously, the use of external technologies demonstrates deepened international collaboration in space technology, which may raise concerns about the dual-use potential of these technologies. In recent years, Iran has placed greater emphasis on the deployment of military satellites, likely in response to increasing geopolitical tensions and the need to enhance its surveillance capabilities.

Discussion: Benefits of the Space Program for Iran's Security Strategy

Iran's space program plays a critical role in achieving the nation's strategic goals, integrating political, economic, military, and scientific dimensions. It represents Tehran's ambitions to reduce dependence on foreign technologies, build national technological capabilities, and bolster its position on the international stage. The development of space technologies enables Iran to enhance its capabilities in communication, Earth observation, and navigation, directly impacting national security and intelligence operations. Furthermore, investments in the space sector drive economic growth by fostering innovation, creating jobs, and promoting collaboration between industry and academia.

Several key aspects of Iran's space program are essential for understanding its contributions to the country's security strategy. These include not only military security but also broader areas such as internal, political, environmental, and technological security.

Environmental Security

Low Earth orbit (LEO) satellites, due to their lower costs and greater accessibility, are a key tool for Iran in building a system to monitor its natural environment. They provide independence from external providers and facilitate the development of domestic technological infrastructure, which is crucial for the nation's strategic security.[47]

Climate change poses undeniable challenges for Middle Eastern countries, particularly Iran. In terms of total greenhouse gas (GHG) emissions, Iran ranks as the largest contributor to climate change in the Middle East and seventh globally.[48] Iran's high GHG emissions are driven by extensive oil and gas production and rapid urbanization.[49] Over the coming decades, the country is projected to experience a 2.6°C increase in average temperatures and a 35% reduction in precipitation.[50] Furthermore, several researchers predict that by the end of the century, heatwaves in Iran and Western Asia will intensify by 30%.[51]

Iran's recent focus on research and the use of remote sensing for environmental monitoring is pivotal for ensuring environmental security. LEO satellites provide regular data on climate changes, such as droughts, floods, and rainfall patterns. This data is critical for managing water resources, forecasting droughts, and optimizing irrigation systems in a country grappling with water scarcity and agricultural degradation.[52] Satellites can also monitor air, water, and soil pollution, enabling the identification of contamination sources and assessing their environmental impact. For a nation battling urban smog and water pollution, these capabilities are vital for policymaking and industrial regulation.[53]

Furthermore, LEO satellites facilitate rapid detection and analysis of natural disasters, such as earthquakes, floods, landslides, and sandstorms, which frequently

47 See more: J.L. Awange, *Environmental Monitoring using GNSS*, New York 2012; V Tramutoli, *Robust Satellite Techniques (RST) for Natural and Environmental Hazards Monitoring and Mitigation: Theory and Applications*, International Workshop on the Analysis of Multi-temporal Remote Sensing Images, Leuven, Belgium 2007, pp. 1–6.

48 M.R.M. Daneshvar, M. Ebrahimi, H. Nejadsoleymani, An overview of climate change in Iran: Facts and statistics, *Environmental Systems Research*, 2019, 8(7), p. 3.

49 V. Karimi, E. Karami, M Keshavarz, Climate change and agriculture: Impacts and adaptive responses in Iran, *Journal of Integrative Agriculture*, 2018, 17(1), p. 5.

50 Iran's Third National Communication to United Nations Framework Convention on Climate Change (UNFCCC), 2017, https://unfccc.int/sites/default/files/resource/Third%20National%20communication%20IRAN.pdf (accessed: 02/02/2025).

51 X. Zhang (et. al), Trends in Middle East climate extremes indices during 1930–2003, *Geophysical Research*, pp. 1–12; F. Rahimzadeh, A. Asgari, E. Fattahi, Variability of extreme temperature and precipitation in Iran during recent decades, *International Journal of Climatology*, 2009, 29(3), pp. 329–343.

52 M.J. Amiri, S.S. Eslamian, Investigation of climate change in Iran, *Journal of Environmental Science and Technology*, 2010, 3(4), pp. 210–212.

53 K.C. Abbaspour, M. Faramarzi, S.S. Ghasemi, H. Yang, Assessing the impact of climate change on water resources in Iran, *Water Resources Research*, 2009, 45(10), https://agupubs.onlinelibrary.wiley.com/doi/full/10.1029/2008WR007615 (accessed: 02/02/2025).

affect Iran.[54] This capability enables quicker responses, minimizing human and material losses. Satellites also support biodiversity management by monitoring deforestation, crop conditions, and soil erosion, essential for a country where agriculture plays a significant economic role.

Technological Security and Critical Infrastructure Resilience

Since the 1979 Islamic Revolution, Iran's prolonged exposure to international sanctions has compelled the nation to explore alternative paths for economic and technological development. One prominent example of Iran's technological resilience is the National Information Network (*Shabake-ye Melli-ye Ettelāʾāt*, SME), a domestic intranet designed to ensure independent communication and internet access.[55]

Iran has also developed a suite of domestic software and hardware solutions to circumvent restrictions on international applications. These include indigenous operating systems (*Ghasedak*, *Sharif Linux*), email services (*Chaapaar*), search engines (*Fajr*, *Parsijoo*), e-commerce platforms (*Digikala*), and social media networks (*Cloob*). The country produces essential IT components, including data centers, routers, microprocessors, and communication devices.[56]

The space program plays a crucial role in bolstering Iran's technological security by reducing reliance on foreign suppliers, fostering the domestic technology sector, and mitigating international pressures. Developing a space program requires mastery of key components such as launch vehicles, satellites, communication systems, and ground stations. This enables Iran to establish independent

54 H. Bahrainy, Natural Disaster Management in Iran during the 1990s—Need for a New Structure, *Journal of Urban Planning and Development*, 2003, 129(3); K. Jahangiri, Y.O. Izadkhah, S.J. Tabibi, A comparative study on community-based disaster management in selected countries and designing a model for Iran, *Disaster Prevention and Management,* 2011, 20(1); K. Zarea, S. Beiranvand, P. Sheini-Jaberi, A. Nikbakht-Nasrabadi, Disaster nursing in Iran: Challenges and opportunities, *Australasian Emergency Nursing Journal*, 2014, 17(4).

55 See also: B. Rahimi, Censorship and the Islamic Republic: Two modes of regulatory measures for media in Iran, *The Middle East Journal*, 2015, 69(3); N. Bajoghli, *Digital Technology as Surveillance*, Routledge 2014; A. Yalcintas, N. Alizadeh, *Digital Protectionism and National Planning in the Age of the Internet: The Case of Iran*, Cambridge University Press 2020; C. Anderson, *The Hidden Internet of Iran: Private Address Allocations on a National Network*, 2012, https://arxiv.org/abs/1209.6398; R. Taghipour, M. Ramek, The strategic model of security analysis in the national information network of I.R. Iran, *Quarterly Journal Strategic Studies in Cyberspace*, 2022, 2(3).

56 M. Stachoń, Iranian cyber capabilities as a tool of domestic and foreign policy, *Scientific Reports of Fire University*, 2024, 2(89), pp. 278–279.

technological standards and reduce the need to import technology subject to export controls or sanctions.

Additionally, the program stimulates private sector growth and strengthens collaboration between universities and research institutions, driving advancements in engineering, electronics, materials science, and IT systems. This enhances national technological capacity, generates employment, and supports overall economic development.

By achieving advanced technological capabilities, Iran could potentially offer its space technologies to other countries, thereby fostering diplomatic and economic relations. Such achievements enhance Iran's negotiating position on the global stage, demonstrating its ability to thrive despite sanctions and isolation.

Political Security and Regime Stability

A key determinant of Iran's security strategy, both domestically and internationally, is the regime's concern for survival. Guided by the ideological principles of the Islamic Revolution, Iranian authorities perceive constant threats from internal factors, such as social unrest, economic crises, and opposition movements, as well as external pressures, including international sanctions, military threats, and geopolitical rivalries. The regime's drive for survival shapes Tehran's strategic decisions, focusing on strengthening its security apparatus, societal control, and the development of asymmetric capabilities such as cyber operations and its missile program.[57]

The development of the space program enhances the state's ability to address challenges posed by opposition activities, providing tools for more effective societal control. Already, under the pretext of combating heresy, anti-Islamism, or defending state interests and the virtues of its citizens, the Iranian government is active in the digital sphere. One method of controlling information is the harassment of activists online and conducting cyberattacks on their social media accounts.[58] Additionally, the government uses information against dissidents to dominate social and political discourses and discredit them in the eyes of the global public.

A relatively new method employed by the Iranian government to manage outbreaks of social unrest and counter anti-government activities online is mass internet shutdowns.[59] The regime also possesses far more precise and sophisticated tools for controlling public opinion. In 2022, evidence surfaced indicating that

57 *Ibidem*.

58 S. Kargar, A. Rauchfleisch, State-aligned trolling in Iran and the double-edged affordances of Instagram, *New Media & Society*, 2019, 21(7), pp. 1510–1511.

59 M. Kazemi, *#Internet Shutdown Trends in Iran: November 2019 to July 2021,* Filterwatch. https://filter.watch/en/2021/09/03/internet-shutdown-trendsin-iran-from-november-2019-to-july-2021/ (accessed: 02/02/2025).

Iran uses surveillance software (*Samane-je Yekparche-je Este'lamat-e Muchabarati*, SIEM) to track and control its citizens, particularly during public protests.[60]

The development of the space program could significantly enhance the regime's societal control capabilities by equipping the government with technological tools to monitor, manage, and suppress opposition activities as well as the general populace. Low Earth orbit (LEO) satellites enable the tracking of population movements, public gatherings, protests, and activities in critical urban and rural areas. This data can be used to rapidly identify and counter opposition activities. High-resolution imaging allows the authorities to monitor strategic sites, such as universities, workplaces, or places of worship, which may serve as hubs for organizing protests.

Moreover, proprietary satellites give the government control over communication systems, including television, radio, and the internet. This control enables the regime to restrict access to content deemed unfavorable while promoting official propaganda and eliminating narratives from independent sources. Satellites can also be used to jam signals from foreign media and satellite internet providers, further limiting citizens' access to alternative viewpoints.

Additionally, satellites can integrate with electronic surveillance systems, enabling geolocation of individuals and devices targeted by operational activities. This is particularly useful for identifying opposition leaders and their supporters.

The space program can also serve as a tool for regime legitimacy and propaganda. Successes in the space program can be used as evidence of the regime's strength and efficiency, reinforcing public belief in the necessity of the current government. Furthermore, showcasing achievements in this area can foster a sense of national pride, diverting attention from internal problems and consolidating support for the ruling authorities.

National Security

As highlighted earlier, Iran's recent focus on military LEO satellites underscores its growing awareness of the strategic advantages offered by space technology in regional and global rivalries. This may indicate a growing awareness within the government of the benefits of leveraging the space program primarily as a strategic advantage over regional and global adversaries.

Preliminary research conducted by the author, yet to be published, indicates that cyber espionage has been the dominant motivation for Iran's advanced persistent threat (APT) groups. Between 2009 and 2024, 41 out of 55 analyzed groups engaged in malicious activities aimed at collecting high-value or classified information. These

60 *Samane-je Yekparcze -je Este'lamat-e Muchabarati* (SIEM), https://www.documentcloud.org/documents/23199209-irans-siam-manual-in-persian-for-tracking-and-controlling-mobile-phones (accessed: 02/02/2025).

cyberattacks targeted critical sectors such as defense, industry, energy, diplomacy, and public administration, encompassing both state entities and private companies, NGOs, and international organizations. The primary objective was to gain intelligence, economic, political, or military advantages, ultimately strengthening Iran's geopolitical position. Cyber espionage also serves as a key tool in the technological race, enabling the theft of advanced technologies, military plans, and industrial innovations, thereby narrowing Iran's technological gap with its competitors.[61]

The development of the space program enhances Iran's intelligence capabilities by providing advanced technologies and tools for data collection and analysis. LEO satellites equipped with optical, radar, or multispectral sensors enable real-time monitoring of ground activities, including troop movements, strategic infrastructure development, and adversarial operations.[62]

Furthermore, in the context of escalating cyber threats and the shift of modern warfare to cyberspace, satellites facilitate the construction of independent, resilient communication systems for the government and military. These systems, integrated with ground infrastructure, can detect cyberattack sources and map adversarial activities in cyberspace. Satellites can also intercept radio signals and satellite communications, supporting sophisticated cyber espionage campaigns.

In summary, Iran's space program significantly bolsters its national security by enhancing intelligence capabilities, ensuring independent communications, and providing tools to counter external and internal threats effectively.

Summary

This article examines the significance of low Earth orbit (LEO) satellites in the (cyber)security strategies of authoritarian states, using Iran as a case study. It focuses on the role of these technologies in areas such as national, technological, environmental, and political security. The study highlights how space technologies, particularly LEO satellites, have become a critical component of authoritarian regimes' security strategies, enabling enhanced internal control, intelligence operations, and the development of independent capabilities in cyberspace.

The article outlines the evolution of Iran's space program, from its inception in the 1950s through the development phases of LEO satellites to contemporary priorities centered on technological autonomy and military capabilities. In Iran's case, the development of the space program aligns with a broader strategy to reduce dependence on foreign technology and data providers, thereby enhancing strategic autonomy.

---

61 Research conducted by the author as part of their doctoral dissertation.

62 See more: C.N. Stevens, Technology in Foreign Intelligence Gathering, *American Intelligence Journal*, 2017, 34(1); J.T. Richelson, *The technical collection of intelligence*, [in:] *Handbook of Intelligence Studies*, Routledge 2006; A. Dupont, *Intelligence for the twenty-first century*, [in:] W.K. Wark (ed.), *Twenty-First Century Intelligence*, Routledge 2005.

LEO satellites play a pivotal role in Iran's security strategy by ensuring independence from foreign suppliers, facilitating environmental monitoring, managing natural resources, and enabling disaster response. They also support technological advancements with dual-use applications in both civilian and military contexts. The article emphasizes the importance of military satellites in bolstering Iran's intelligence capabilities, including monitoring adversaries' troop movements and infrastructure, as well as conducting cyberespionage operations.

Additionally, LEO satellites are integral to maintaining regime security. In the context of political security, they aid the regime in societal control, monitoring protests, and curbing opposition activities. These technologies also enable faster responses to threats such as protests, sabotage, or cyberattacks. Furthermore, LEO satellites support disinformation and propaganda efforts, reinforcing the regime's legitimacy by showcasing technological achievements and restricting access to external information.

The author underscores that the development of domestic space technologies reduces Iran's vulnerability to international sanctions and restrictions on access to foreign satellite services. This strengthens its defensive and offensive capabilities in a rapidly evolving international environment. From a cybersecurity perspective, LEO satellites enable Iran to secure communications, monitor network activity, and conduct offensive operations against adversaries.

In conclusion, the development of Iran's space program represents a vital element of its security strategy. LEO satellites play a critical role in Iran's (cyber) security policies, integrating technological capabilities with the regime's strategic goals in technological, military, and political domains. The article suggests that LEO satellites enhance the regime's control mechanisms, contribute to technological self-sufficiency, and support the realization of long-term strategic objectives. However, they also raise concerns regarding their potential use in escalating regional and global conflicts.

Bibliography

Abbaspour, K.C., **Faramarzi, M.**, **Ghasemi, S.S.**, **Yang, H.**, Assessing the impact of climate change on water resources in Iran, *Water Resources Research*, 2009, 45(10), pp. 1–16. Available at: https://agupubs.onlinelibrary.wiley.com/doi/full/10.1029/2008WR007615 (accessed: 02/02/2025).

Amiri, M.J., **Eslamian, S.S.**, Investigation of climate change in Iran, *Journal of Environmental Science and Technology*, 2010, 3(4), pp. 210–212.

Anderson, C., *The Hidden Internet of Iran: Private Address Allocations on a National Network*, 2012. Available at: https://arxiv.org/abs/1209.6398 (accessed: 02/02/2025).

Andrusiewicz, K.M., Korpus Strażników Rewolucji w systemie politycznym i polityce bezpieczeństwa Islamskiej Republiki Iranu, *Rocznik Bezpieczeństwa Wewnętrznego*, 2012/2013, pp. 361–362.

Awange, J.L., *Environmental Monitoring using GNSS*, New York 2012.

Bahrainy, H., Natural Disaster Management in Iran during the 1990s—Need for a New Structure, *Journal of Urban Planning and Development*, 2003, 129(3), pp. 1–20.

Bajoghli, N., *Digital Technology as Surveillance*, Routledge 2014.

Daneshvar, M.R.M., **Ebrahimi, M.**, **Nejadsoleymani, H.**, An overview of climate change in Iran: Facts and statistics, *Environmental Systems Research*, 2019, 8(7), pp. 1–10.

Dupont, A., *Intelligence for the Twenty-First Century*, [in:] W.K. Wark (ed.), *Twenty-First Century Intelligence*, Routledge 2005.

Harvey, B., **Smid, H.H.F.**, **Pirard, T.**, *Emerging Space Powers. The New Space Programs of Asia, the Middle East, and South America*, Chichester 2010.

Iran's Third National Communication to United Nations Framework Convention on Climate Change (UNFCCC), 2017. Available at: https://unfccc.int/sites/default/files/resource/Third%20National%20communication%20IRAN.pdf (accessed: 02/02/2025).

Iranian Space Agency. Available at: https://www.undrr.org/organization/iranian-space-agency (accessed: 02/02/2025).

Iranian Space Agency, *History of Iranian Space Agency*, 21 August 2019 (30 Mordad 1398 SH). Available at: https://web.archive.org/web/20210730123140/https://isa.ir/fa/general_content/41505-%D8%AA%D8%A7%D8%B1%D-B%8C%D8%AE%DA%86%D9%87.html (accessed: 02/02/2025).

***Iranian Space Organization (Sazeman-e Fazayi Iran)*, Ministry of Communications and Information Technology**. Available at: https://web.archive.org/web/20080607133426/http://www.ict.gov.ir/companies-ministry-space-fa.html (accessed: 02/02/2025).

Iranian Space Research Center, *About*. Available at: https://web.archive.org/web/20220201170828/https://www.isrc.ac.ir/%D8%AF%D8%B1%D8%A8%D8%A7%D8%B1%D9%87-%D9%BE%DA%98%D9%87%D8%B4%DA%AF%D8%A7%D9%87 (accessed: 02/02/2025).

IRGC-Air Force Al-Ghadir Missile Command, *Iran Watch*, Wisconsin Project on Nuclear Arms Control, March 2, 2011. Available at: https://www.iranwatch.org/iranian-entities/irgc-air-force-al-ghadir-missile-command (accessed: 02/02/2025).

Islamic Revolutionary Guard Corps (IRGC) Aerospace Force Self-Sufficiency Jihad Organization, *Iran Watch*, Wisconsin Project on Nuclear Arms Control, 24 February 2023. Available at: https://www.iranwatch.org/iranian-entities/islamic-revolutionary-guard-corps-irgc-aerospace-force-self-sufficiency-jihad-organization (accessed: 02/02/2025).

Islamic Revolutionary Guard Corps (IRGC) Aerospace Force, *Iran Watch*, Wisconsin Project on Nuclear Arms Control, 24 August 2020. Available at: https://www.iranwatch.org/iranian-entities/islamic-revolutionary-guard-corps-irgc-aerospace-force (accessed: 02/02/2025).

Islamic State of Iran, **The Act on the Establishment of the Iranian Remote Sensing Center**, 6 October 1991 (14 Mehr 1370 SH). Available at: https://rc.majlis.ir/fa/law/show/91955 (accessed: 02/02/2025).

Islamic State of Iran, **The Constitution of the Islamic Revolutionary Guard Corps (Asasname-ye Sepah-e Pasdaran-e Enghelab-e Eslami)**, 6 September 1982 (15 Shahrivar 1361). Available at: https://rc.majlis.ir/fa/law/show/90595 (accessed: 02/02/2025).

Islamic State of Iran, **The Constitution of the Islamic State of Iran**, Article 150 (Qanun-e Asasi-ye Jomhuri-ye Eslami-ye Iran). Available at: https://rc.majlis.ir/fa/law/show/132239

Jahangiri, K., **Izadkhah, Y.O.**, **Tabibi, S.J.**, A comparative study on community-based disaster management in selected countries and designing a model for Iran, *Disaster Prevention and Management,* 2011, 20(1), pp. 82–94.

Kargar, S., **Rauchfleisch, A.**, State-aligned trolling in Iran and the double-edged affordances of Instagram, *New Media & Society*, 2019, 21(7), pp. 1510–1511.

Karimi, V., **Karami, E.**, **Keshavarz, M.**, Climate change and agriculture: Impacts and adaptive responses in Iran, *Journal of Integrative Agriculture*, 2018, 17(1), pp. 1–15.

Kazemi, M., *#Internet Shutdown Trends in Iran: November 2019 to July 2021*, Filterwatch. Available at: https://filter.watch/en/2021/09/03/internet-shutdown-trendsin-iran-from-november-2019-to-july-2021/

Krzyzaniak, J., *Part 1: Explainer—Iran's Space Program*, *The Iran Primer*, United States Institute of Peace, 9 August 2022. Available at: https://iranprimer.usip.org/blog/2022/jun/03/explainer-irans-space-program

Mesbah 1., *Gunter's Space Page*. Available at: https://space.skyrocket.de/doc_sdat/mesbah-1.htm (accessed: 02/02/2025).

Rahimi, B., Censorship and the Islamic Republic: Two modes of regulatory measures for media in Iran, *The Middle East Journal*, 2015, 69(3), pp. 358–378.

Rahimzadeh, F., **Asgari, A.**, **Fattahi, E.**, Variability of extreme temperature and precipitation in Iran during recent decades, *International Journal of Climatology*, 2009, 29(3), pp. 329–343.

Richelson, J.T., *The Technical Collection of Intelligence*, [in:] *Handbook of Intelligence Studies*, Routledge 2006.

Shapir, Y.S., Iran's efforts to conquer space, *The Institute for National Security Studies Strategic Assessment*, 2005, 8(3), pp. 7–12.

Stachoń, M., Iranian cyber capabilities as a tool of domestic and foreign policy, *Scientific Reports of Fire University*, 2024, 2(89), pp. 278–279.

Statute of the Iranian Space Agency, 13 June 2008 (24 Khordad 1387 SH). Available at: https://rc.majlis.ir/fa/law/show/134694 (accessed: 02/02/2025).

Stevens, C.N., Technology in Foreign Intelligence Gathering, *American Intelligence Journal*, 2017, 34(1), pp. 123–130.

Taghipour, R., **Ramek, M.**, The strategic model of security analysis in the national information network of I.R. Iran, *Quarterly Journal Strategic Studies in Cyberspace*, 2022, 2(3), pp. 1–10.

Tarikhi, P., Statutes of the Iranian Space Agency, *Journal of Space Law*, 2008, 34(2), pp. 3–7.

Tramutoli, V., *Robust Satellite Techniques (RST) for Natural and Environmental Hazards Monitoring and Mitigation: Theory and Applications*, International Workshop on the Analysis of Multi-temporal Remote Sensing Images, Leuven, Belgium 2007.

United Nations, *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*, General Assembly resolution 34/68. Available at: https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/moon-agreement.html (accessed: 02/02/2025).

United Nations, *Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space*, General Assembly resolution 2345 (XXII). https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/rescueagreement.html (accessed: 02/02/2025).

United Nations, *Agreement relating to the International Telecommunications Satellite Organization 'INTELSAT'* (with annexes). Available at: https://treaties.un.org/Pages/showDetails.aspx?objid=08000002800e8e08&clang=_en (accessed: 02/02/2025).

United Nations, Committee on the Peaceful Uses of Outer Space: Membership Evolution. Available at: https://www.unoosa.org/oosa/en/ourwork/copuos/members/evolution.html (accessed: 02/02/2025).

United Nations, *Convention on International Liability for Damage Caused by Space Objects*, General Assembly resolution 2777 (XXVI).

United Nations, *Convention on Registration of Objects Launched into Outer Space*, General Assembly resolution 3235 (XXIX).

United Nations, *Treaty 2222 (XXI) on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*.

Wehrey, F., **Green, J.D.**, **Nichiporuk, B.**, **Nader, A.**, **Hansell, L.**, **Nafisi, R.**, **Bohandy, S.R.**, *The Rise of the Pasdaran: Assessing the Domestic Roles of Iran's Islamic Revolutionary Guards Corps*, RAND Corporation, 2009, pp. XI–XVIII. Available at: https://www.rand.org/content/dam/rand/pubs/monographs/2008/RAND_MG821.pdf (accessed: 02/02/2025).

Yalcintas, A., **Alizadeh, N.**, *Digital Protectionism and National Planning in the Age of the Internet: The Case of Iran*, Cambridge University Press, 2020.

Zarea, K., **Beiranvand, S.**, **Sheini-Jaberi, P.**, **Nikbakht-Nasrabadi, A.**, Disaster nursing in Iran: Challenges and opportunities, *Australasian Emergency Nursing Journal*, 2014, 17(4), pp. 190–196.

Zhang, X. et al., Trends in Middle East climate extreme indices from 1950 to 2003, *Geophysical Research*, 110(D22), pp. 1–12.

https://doi.org/10.18778/8331-719-9.11

How Starlink Has Impacted Connectivity Initiatives in Africa

Jason Bonsall[1]

Introduction

Africa endures the most profound impacts of the global digital divide, grappling with severe connectivity challenges. According to the International Telecommunication Union (ITU), 23% of individuals in rural areas in Africa use the Internet, the lowest percentage of any other region as of 2023. Comparatively, 57% of Africa's urban population is connected to the Internet. As reported by the ITU, Africa's 2.49 urban-to-rural Internet access ratio is the largest disparity out of any other region.[2] The ITU's figures display that providing Internet access to rural African regions is a key challenge in any global effort to connect the world to the Internet. Despite these access problems in rural areas, affordability has consistently been identified as the primary obstacle to connecting Africa's population to the Internet. In two surveys by Research ICT Africa, affordability is a "longstanding challenge".[3] The GSM Association (GSMA), a non-profit organisation working with mobile network operators to support innovation and increase connectivity, discovered that in Sub-Saharan Africa, an entry-level device costs 95% of the average monthly income for the poorest 20% of the population. A different study by the GSMA showed that in 2022, over half of Sub-Saharan African countries did not meet the affordability baseline

1 Fellow, Trusted Internet Summer School on Internet Governance and International Law, Poland.

2 International Telecommunication Union, *Statistics*, 2024. Available at: https://www.itu.int/en/ITU-D/Statistics/pages/stat/default.aspx (accessed: 21/10/2024).

3 Ch. Chair, Internet Use Barriers And User Strategies: Perspectives from Kenya, Nigeria, South Africa and Rwanda, *Research ICT Africa, Beyond Access Policy Paper*, 2017, 1; Internet Use Barriers And User Strategies: Perspectives From Kenya, Nigeria, South Africa And Rwanda, *Research ICT Africa, Beyond Access Policy Paper* 2017, p. 7.

when averaging the income of the whole population. When averaging the income of the bottom 40% of the population, the GSMA finding revealed that over 60% of countries in Sub-Saharan Africa met this target.[4] Any effort to connect the world's population to the Internet must focus on Africa. More specifically, this effort must prioritise the service's affordability and access in rural areas in Africa.

Since the late 1990s, there have been attempts to utilise satellites to provide global high-speed, affordable Internet connectivity. In many early iterations, such as Hughes Network Systems (Hughesnet), the speed was slower than that of a terrestrial connection, so their clients preferred terrestrial networks.[5] Most early efforts placed their satellites in Geosynchronous Earth Orbit (GSO), meaning they were orbiting 35,786 km from Earth's equator.[6] For satellite Internet companies to offer a connection comparable to terrestrial Internet Service Providers (ISPs), their satellites must be in Low Earth Orbit (LEO), from 80–100 km to 2,000 km.[7] This is where Starlink deployed its space-based infrastructure and emerged as a formidable competitor in the market. Some experts suggest that Starlink's entry into the ICT (Information and Communications Technology) market coincides with a period when monopolistic structures were producing undesirable effects in the telecommunications markets of several countries.[8] Starlink and other LEO satellite broadband companies can create competition in this market, and a competitive market can benefit consumers by making Internet access more affordable. Therefore, LEO satellite technology can potentially solve critical connectivity challenges in Africa by connecting rural areas to the Internet and competing with entrenched monopolies.

Numerous connectivity initiatives in Africa are looking at creative ways to bring connectivity to the continent. This chapter examines two connectivity initiatives geared toward achieving the same goal and represents different approaches. One is led by United Nations (UN) agencies, and the other by a consortium of private companies. These heavily funded initiatives represent private and intergovernmental models. Starlink, a private company that relies heavily on government

4 M. Shanahan, K. Bahla, *The State of Mobile Internet Connectivity 2024*, Global System for Mobile Communications Association, London 2024, p. 5. Available at: https://www.gsma.com/r/wp-content/uploads/2024/10/The-State-of-Mobile-Internet-Connectivity-Report-2024.pdf (accessed: 21/10/2024).

5 J.V. Evans, The Proposed Ku-Band Non Geostationary Communication Satellite Systems, *Space an Integral Part of the Information Age*, 2000, 47(2), pp. 171–182, https://doi.org/10.1016/S0094-5765(00)00057-6; S. Liu, Z. Gao, Y. Wu, D. W. Kwan Ng, X. Gao, K. -K. Wong, S. Chatzinotas, B. Ottersten, LEO satellite constellations for 5G and beyond: How will they reshape vertical domains? *IEEE Communications Magazine*, 2021, 59(7), pp. 30–36, https://doi.org/10.1109/MCOM.001.2001081

6 A. Capannolo, S. Silvestrini, A. Colagrossi, V. Pesce, *Chapter Four—Orbital Dynamics*, [in:] V. Pesce, A. Colagrossi, S. Silvestrini (eds.), *Modern Spacecraft Guidance, Navigation, and Control*, Elsevier, 2023, pp. 131–206, https://doi.org/10.1016/B978-0-323-90916-7.00004-4

7 H. Riebeek, *Catalog of Earth Satellite Orbits*, National Aeronautics and Space Administration, Washington D.C. 2009. Available at: https://earthobservatory.nasa.gov/features/OrbitsCatalog (accessed: 02/02/2025).

8 S. Liu et al., *op. cit*.

support, falls between these two approaches. In this context, this essay aims to answer two key questions raised by the growing number of initiatives aimed at expanding global Internet access and the capability of LEO satellites to provide worldwide connectivity. First, why have more connectivity initiatives and countries not adopted Starlink? Second, what impact has Starlink had on LEO satellite Internet services in African nations?

Background: Achieving Universal Meaningful Digital Connectivity by 2030

The goal of the International Telecommunications Satellite Organization (ITSO) is to "ensure that poor and underserved «lifeline connectivity» nations remain connected to the outside world".[9] In fulfilling this goal, at the Geneva 2004 World Summit on Information Society (WSIS) summit, the ITSO proposed its Global Broadband Satellite Infrastructure Initiative (GBSI). The ITSO envisioned the GBSI following the same model as the European Global Standards for Mobile Communications (GSM). Therefore, the ITSO would coordinate a public-private partnership to combine resources and reduce regulatory requirements to develop one constellation of satellites and user hardware to promote closing the digital divide.[10] If executed correctly, it would lead to collectively creating and maintaining one infrastructure for satellite broadband services that would reduce the cost to users and regulatory requirements for the companies. This collective focus eventually diminished, and the ITSO's GBSI has been eclipsed by private ventures such as Starlink.

In 2021, a multistakeholder consultation on the UN Secretary-General's Roadmap for Digital Cooperation resulted in a document titled *Achieving Universal and Meaningful Digital Connectivity: Setting a Baseline and Targets for 2030*.[11] This document, written by the Office of the Secretary-General's Envoy on Technology (OSET) and the ITU, outlines steps the UN will take to ensure everyone has "safe and affordable access to the Internet by 2030." As the data shared in the introduction section shows, Africa requires special attention in any global connectivity

9 K. Katkin, The global broadband satellite infrastructure initiative, *SSRN*, 2006, pp. 1–49. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103932*The Global Broadband Satellite Infrastructure Initiative,* The 34th Research Conference on Communication Information and Internet Policy, 2006, p. 2. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103932 (accessed: 02/02/2025).

10 *Ibidem*.

11 International Telecommunication Union & Office of the Secretary-General's Envoy on Technology, *Achieving universal and meaningful digital connectivity: Setting a baseline and targets for 2030*, United Nations, 2021. Available at: https://www.itu.int/itu-d/meetings/statistics/wp-content/uploads/sites/8/2022/04/UniversalMeaningfulDigitalConnectivityTargets2030_BackgroundPaper.pdf (accessed: 02/02/2025).

vision. The ITU's analysis of the urban-rural gap states that it has barely improved from 2020 to 2023 and the "digital divide across income groups is magnified in rural areas".[12] In 2023, an ITU press release concluded that "current trends are not strong enough to guarantee that the objective of universal, meaningful connectivity will be met by 2030".[13] The lack of sufficient progress on their objectives to achieve Universal Meaningful Connectivity by 2030 implies that there should be shifts in the ITU and OSET's strategies for achieving this target. Given the ITU's stated intent to collaborate with the private sector, should the ITU integrate Starlink and its emerging competitors in its efforts to reach its target? This is explored in Section V concerning Starlink's policy and regulatory challenges.

Connectivity Initiatives in Africa

A project led by Meta and a consortium of seven other ICT companies from various countries, 2Africa's goal is to "significantly increase the capacity, quality, and availability of Internet connectivity between Africa and the rest of the world".[14] The consortium explained that it focused on Africa because its Internet penetration consistently fell below the global average. Additionally, they state that this project will help African countries meet many of the Sustainable Development Goals (SDGs) that rely on Internet connectivity.[15]

This project's stated intentions appear altruistic, yet its critics perceive it as an attempt by companies to exploit developing countries for profit rather than provide genuine assistance. Mwema and Birhane associate this project with "The new frontiers of digital colonialism".[16] These authors see 2Africa as a ploy to create "Infrastructure Debt," where African countries continually pay for connection to the Internet through private infrastructure. They have found that these companies can construct this cable and provide this service "with no oversight and little transparency".[17] Ultimately, these authors argue that 2Africa is exploiting the international push for universal digital connectivity for its financial gain and hiding behind the guise of SDGs.

---

12 International Telecommunication Union, *Statistics*. Available at: https://www.itu.int:443/en/ITU-D/Statistics/pages/stat/default.aspx (accessed: 02/02/2025).

13 International Telecommunication Union, *Population of global offline continues steady decline to 2.6 billion people in 2023*, 2024. Available at: https://www.itu.int/en/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx (accessed: 02/02/2025); International Telecommunications Union, *Population of Global Offline Continues Steady Decline to 2.6 Billion People in 2023*, "Press Release", Sept. 12, 2024. Available at: https://www.itu.int:443/en/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx (accessed: 02/02/2025).

14 2Africa, About |. 2Africa Cable2Africa Deployment Is Underway. 2Africa Is Now Landing across 3 Continents and Will Be Ready for Service in Most Places as Early as 2023, *2Africa Cable*, 2022. Available at: https://www.2africacable.net/about (accessed: 02/02/2025).

15 *Ibidem*.

16 E. Mwema, A. Birhane, Undersea Cables in Africa: The New Frontiers of Digital Colonialism, *First Monday*, 2024, 29(4), p. 1.

17 *Ibidem*.

The ITU & OSET-led initiative, 2Africa, and numerous other initiatives stem from a shared vision for the continent and a recognition of the urgent need to bridge the digital divide. The former includes more stakeholders and must comply with internationally established statutes and standards. The latter shows how it is not beholden to as much red tape but receives heavy pushback from scholars and activists. Starlink should be seen as an attempt to navigate between these two different types of initiatives, aiming to reap the benefits of both.

Overview of Starlink

Starlink, a division of Space Exploration Technologies Corp. (SpaceX), is a satellite Internet service that utilises LEO satellites to deliver high-speed, low-latency Internet to users worldwide. Technically described as a constellation, Starlink consists of thousands of inter-operating satellites orbiting 550 km from Earth. According to Astronomer Jonathan McDowell, who tracks and publishes the constellation on his private website, there were 6,441 total working Starlink satellites in this low earth orbit as of October 24, 2024.[18] Due to the low altitude of these satellites, information communicated between ground stations, satellites, and users leads to lower latency and faster Internet.[19] Starlink's speed and low latency are comparable to commercial terrestrial Internet service providers.

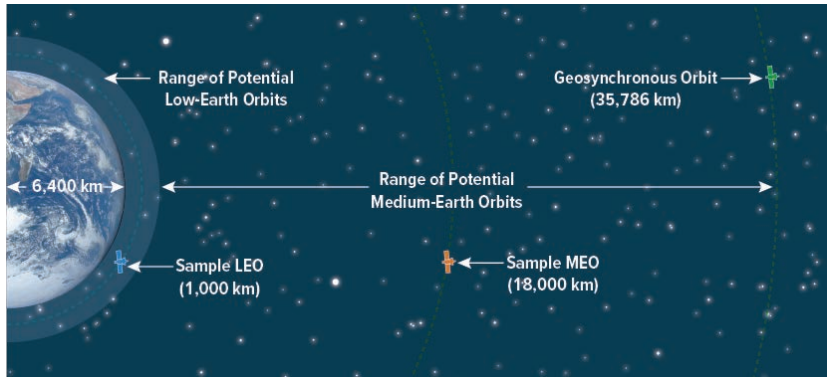


Fig. 1. Low Earth Orbit (LEO), Medium-Earth Orbits (MEO), and Geostationary Orbit (GEO) Satellite Communications System

Source: M. Bennett, C. Kramer, *Large Constellations of Low-Altitude Satellites: A Primer*, Congressional Budget Office, 2023. Available at: https://www.cbo.gov/publication/58794 (accessed: 02/05/2025).

18 J. McDowell, *Jonathan's Space Pages: Starlink Statistics – Starlink Launch Statistics*. Available at: https://planet4589.org/space/con/star/stats.html (accessed: 24/10/2024).

19 A. Yadav, A. Manthan, A. Somya, V. Sachin, *Internet From Space Anywhere and Anytime – Starlink,* 2nd International Conference on "Advancement in Electronics & Communication Engineering", 2022, pp. 480–487. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4160260 (accessed: 24/10/2024).

LEO Internet satellites serve as a junction transmitting information to and from user hardware and a ground station connected to fibre optic cables. Due to the constellation being relatively low in altitude, the satellites orbit Earth at faster speeds.[20] Therefore, to provide consistent coverage, LEO Internet constellations must coordinate their trajectory so that when one satellite falls out of range, another satellite can support that connection. This means constellations, such as Starlink, require thousands of satellites orbiting at all times.

Data transmission through satellite broadband networks is conducted through uplinks, downlinks, and crosslinks. When a user transfers information through an Internet search to a satellite, it is called an uplink. Satellites transferring information to one another are called crosslinks. Finally, the downlink is the ground station and satellites' response to the user's request.[21] The speed for information to travel between these links is characterised by megabits per second (Mbps).

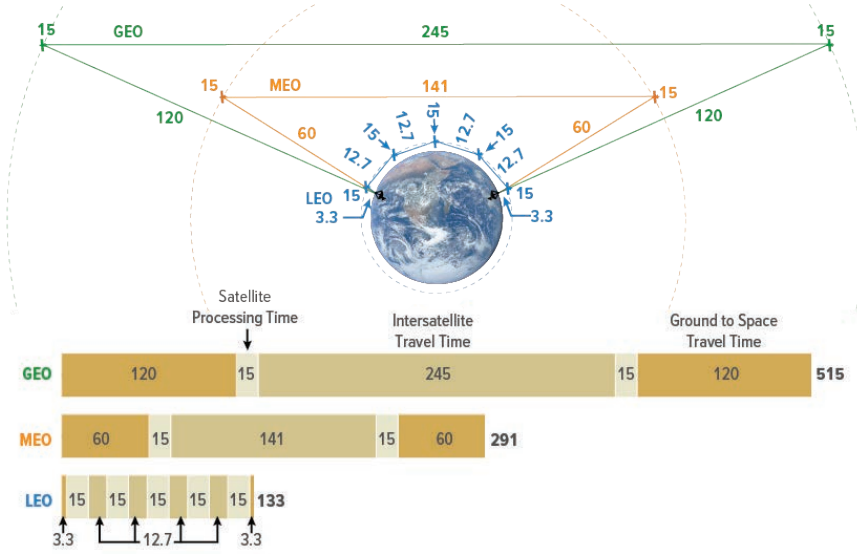


Fig. 2. Time to Transmit a Signal 13,000 Kilometers Across Earth's Surface (in Milliseconds)
Source: M. Bennett, C. Kramer, *Large Constellations of Low-Altitude Satellites: A Primer*, Congressional Budget Office, 2023. Available at: https://www.cbo.gov/publication/58794 (accessed: 02/05/2025).

20 The speed at which LEO satellites travel subsequently requires multiple satellites to coordinate while providing network connection to its users. Starlink satellites, for example, move at around 17,000 miles per hour and circle Earth in ninety minutes (Feldstein, 2024)

21 S. Weston (ed.), *Small Spacecraft Systems Virtual Institute: Small Spacecraft Technology State-of-the-Art Report*, NASA Ames Research Center, Moffett Field 2024, pp. 243–251. Available at: https://www.nasa.gov/wp-content/uploads/2024/03/soa-2023.pdf?emrc=8ad1a1 (accessed: 24/10/2024).

Figure 2 illustrates the inter-satellite travel time for GEO, MEO, and LEO satellites. This figure shows that LEO satellites have a considerably faster Internet connection than GEO and MEO satellites. LEO satellite constellations are moving so fast that a satellite can connect to a fixed point on Earth for only ten minutes before it moves out of range. Once a satellite moves out of the user's connection range, a new satellite must carry over the duties of the older satellite's information requests from various users.[22] This means that satellites within a constellation must be able to communicate large amounts of information to each other constantly.

Starlink's Global and Regional Rollout

Figures 3 and 4[23] show that Starlink is authorised and licensed to operate in 108 countries and territories.[24] This data shows that Starlink has moved quickly to comply with national regulatory requirements in numerous countries.

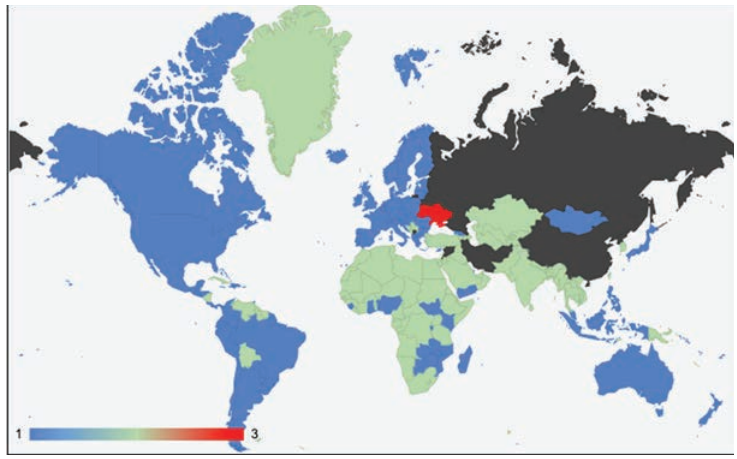


Fig. 3. Map of Starlink Coverage
Source: Starlink, 2024; United Nations Economic Commission for Europe, *UN/LOCODE code list by country and territory*, UNECE, 30 July 2024. Available at: https://unece.org/trade/cefact/unlocode-code-list-country-and-territory; Legend: Covered= Blue, Coming Soon= Green, Waitlist = Red, No Coverage = Black.

22 B. Akcali Gur, J. Kulesza, Equitable Access to Satellite Broadband Services: Challenges and Opportunities for Developing Countries, *Telecommunications Policy*, 2024, 48(5), pp. 1–10, https://doi.org/10.1016/j.telpol.2024.102731; M. Bennett, C. Kramer, *Large Constellations of Low-Altitude Satellites: A Primer*, Congressional Budget Office, 2023. Available at: https://www.cbo.gov/publication/58794 (accessed: 02/05/2025).

23 Waitlisted Countries and Territories include Ukraine, Pitcairn, Saint Helena, Bouvet Island and Singapore.

24 Starlink, *Availability Map*. Available at: https://www.starlink.com/map (accessed: 27/10/2024); UNECE, *UN/LOCODE Code List by Country and Territory*, Jul. 30, 2024. Available at: https://unece.org/trade/cefact/unlocode-code-list-country-and-territory (accessed: 26/10/2024).

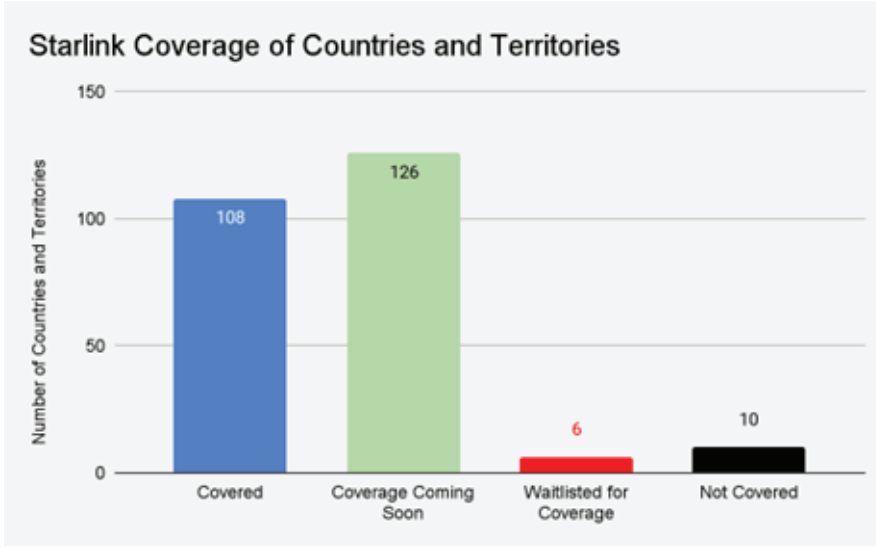


Fig. 4. Starlink Coverage of Countries and Territories
Source: Starlink, *Availability Map*. Available at: https://www.starlink.com/map (accessed: 27/10/2024).

Within Starlink's *Availability Map*, the company explains why a specific country or territory is classified as "Coming Soon," which informs potential customers when they might be able to expect the service and explains why there is a delay in coverage. For each of the one hundred twenty-six countries classified within this map as "Coming Soon," four standard explanations were given for the delay in coverage. These explanations were quantified on how frequently they appear in Figure 5 below and speak to the complexity of these regulatory barriers.

Thirty-eight of these countries and territories listed under the "Coming Soon" classification state that their coverage will begin in 2024, suggesting that the "Coming Soon" classification might not be completely accurate.[25] Furthermore, these figures reveal the regulatory complexity and challenges of obtaining the ability to provide an Internet connection to the world.

25 Five of the thirty-eight countries and territories listed within this classification have additional information explaining that their coverage will begin in "Q4" of 2024. This represents the fourth quarter of the fiscal year, which runs from October 1st to December 31st, meaning that this research took place during this "Q4" period of 2024.

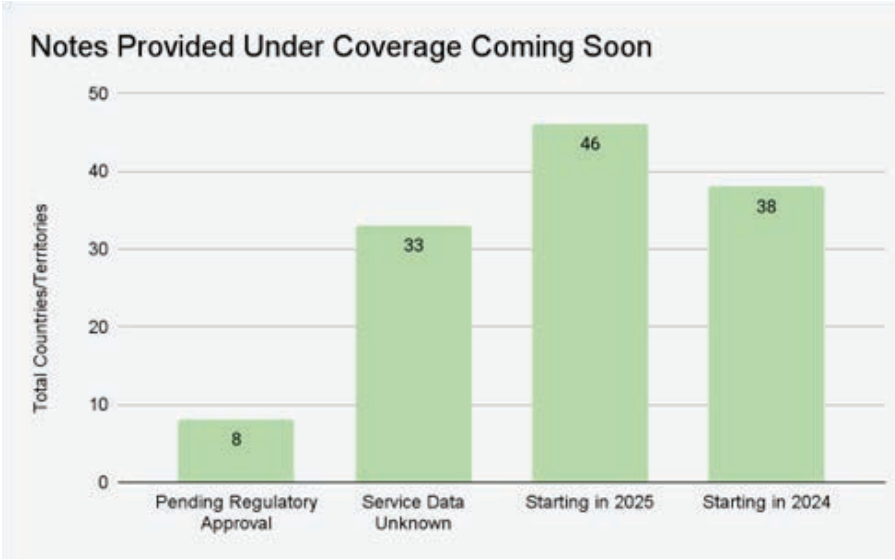


Fig. 5. Notes Provided Under Coverage Coming Soon
Source: Starlink, 2024.

Starlink's Impact on Internet Connectivity in African Countries

Starlink has quickly emerged as a major global Internet service provider (ISP) capable of competing with terrestrial ISPs worldwide. The demand for Starlink's service in Africa can be seen in Starlink's availability map, which shows that they have sold out of their kits in large cities within Nigeria, Zimbabwe, Kenya, Zambia, and Madagascar.[26] Additionally, in April of 2024, Starlink reached an agreement with Jumia, the largest e-commerce platform in Africa, to allow their residential kits to be purchased on Jumia's platform.[27] This example illustrates Starlink's willingness to work with other actors in the African market to increase ease of access to its services. Starlink's speeds, being between 25 and 220 Mbps, significantly outperform the average broadband speed for Northern Africa (12.52 Mbps) and Sub-Saharan Africa (14.99 Mbps).[28] Starlink's Internet speed and coverage speak to its ability to satisfy many key "connectivity enablers" in the UN's meaningful connectivity standard for infrastructure.[29]

26 *Ibidem*.

27 F. Awowede, *To win in Nigeria, Starlink cuts price to ₦40k,* "Technology Times", Nov. 4, 2024. Available at: https://technologytimes.ng/starlink-cuts-price-in-nigeria/ (accessed: 09/11/2024); Jumia, *Starlink and Jumia Collaborate to Expand Internet Service in Africa*, Oct. 2, 2023 (accessed: 09/11/2024).

28 D. Howdle, *Worldwide Broadband Speed League 2024,* Cable.co.uk, 30 June 2024. Available at: https://www.cable.co.uk/broadband/speed/worldwide-speed-league/ (accessed: 30/10/2024).

29 International Telecommunication Union & Office of the Secretary-General's Envoy on Technology, *op. cit.*

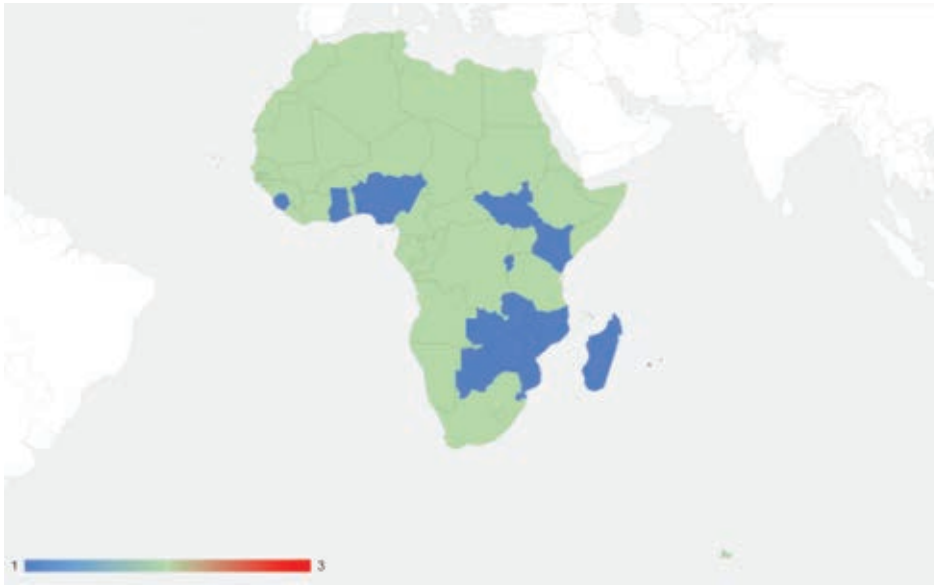


Fig. 6. Starlink Coverage of African Continent; Legend: Covered= Blue, Coming Soon Green, Waitlist = Red, No Coverage = Black.
Source: Starlink, *Availability Map*. Available at: https://www.starlink.com/map (accessed: 27/10/2024).

Starlink's *Availability Map* reveals that out of the fifty-seven African countries and territories, Starlink covers fifteen and is coming soon to the other forty-three. The explanation for the delay in coverage on the availability map stated that "service date is unknown" for all forty-three countries and territories within the "Coming Soon" category.[30] This reveals SpaceX's ambition and commitment to providing coverage across the continent. Nevertheless, the explanation also speaks to various obstacles the company must overcome.

Affordability and Economic Feasibility of Starlink in Africa

When comparing Starlink's average monthly service charge in Africa to the average monthly broadband plan in Africa, as seen in Figure 7, Starlink appears to be addressing the lack of affordability of Internet services in the continent. For example, Mozambique has one of the world's highest average monthly broadband costs, equivalent to $118.26.[31] Starlink, on the other hand, offers its monthly service for the equivalent of $46.96.[32] Comparing these two costs at face value, the choice is evident to a user in Mozambique. A user wanting to establish Starlink as their Internet service provider must also pay for Starlink's hardware. Figure 8 combines

30 Starlink, *Availability Map*.
31 D. Howdle, Global Broadband Pricing League Table 2024.
32 Starlink, *Availability Map*.

the price for a month of Internet service and the hardware cost for each African country that Starlink covers.

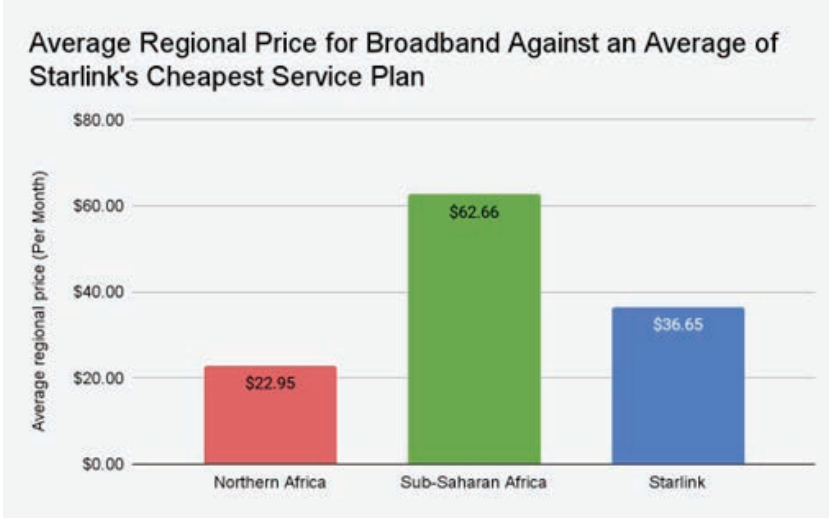


Fig. 7. Average Regional Price for Broadband Against an Average of Starlink's Cheapest Service Plan
Source: Starlink, *Availability Map*. Available at: https://www.starlink.com/map (accessed: 27/10/2024); D. Howdle, *Worldwide Broadband Speed League 2024,* Cable.co.uk, 30 June 2024. Available at: https://www.cable.co.uk/broadband/speed/worldwide-speed-league/ (accessed: 30/10/2024).

Furthermore, consideration must be given to the lifespan of the Starlink hardware, which is all purchased equipment that establishes the customer's internet connection. According to Starlink Specifications, customers should be able to expect their hardware to connect them to the Internet and remain intact and operable for a minimum of 12 or 24 months.[33] These specifications reveal a new reality for users connecting through satellite broadband. Satellite broadband users have intrinsically obtained some responsibility for maintaining a significant part of the infrastructure they rely on to connect them to the Internet. By comparison, users utilising terrestrial ISPs have most of their network connection maintained by the provider, which is factored into their monthly subscriptions.

Therefore, users who see the initial difference in monthly broadband prices advertised in Figure 7 must consider two factors of this coverage. First, users assume responsibility for infrastructure maintenance that would be factored into a monthly subscription to an ISP run through fibre-optic cables. Second, this is an investment in hardware that, according to Starlink, might last one year before it needs to be replaced, even if appropriately maintained.

33 *Ibidem*; Starlink, *Specifications*. Available at: https://www.starlink.com/specifications?spec=5 (accessed: 11/11/2024).

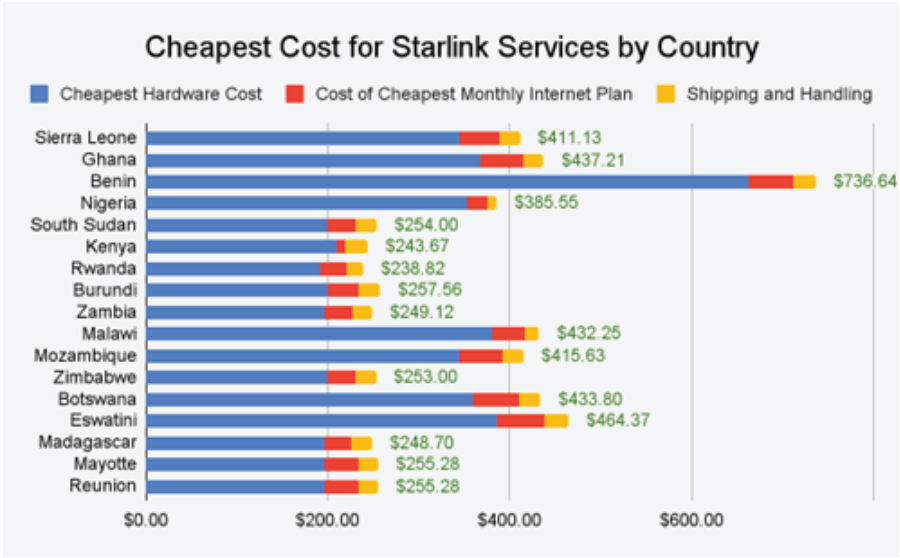


Fig. 8. Cheapest Cost of Starlink Services by Country
Source: Starlink, *Availability Map*. Available at: https://www.starlink.com/map (accessed: 27/10/2024).

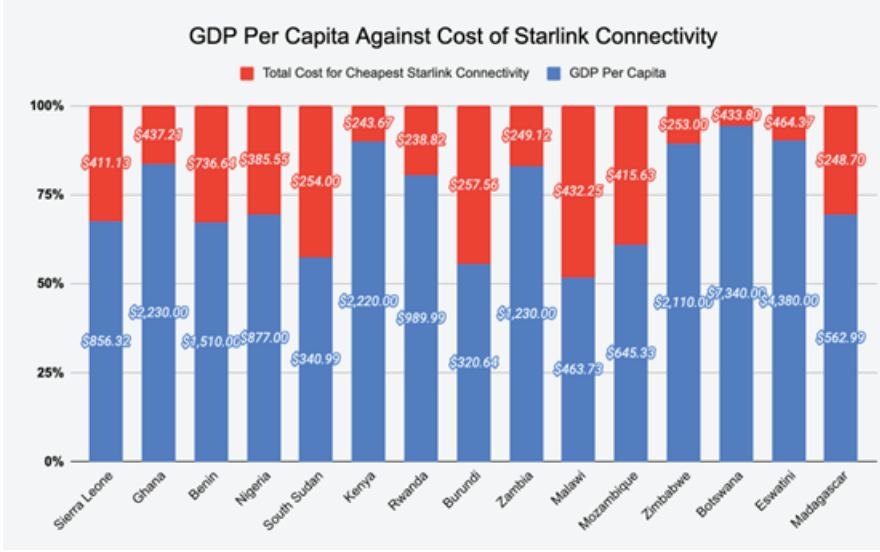


Fig. 9. GDP Per Capita Against Cost of Starlink Connectivity
Sources: Starlink, *Availability Map*. Available at: https://www.starlink.com/map (accessed: 27/10/2024); International Monetary Fund, World economic outlook (October 2024) – GDP per capita, current prices, 2024. Available at: https://www.imf.org/external/datamapper/NGDPDPC@WEO (accessed: 27/10/2024).

To reveal Starlink's economic feasibility to African users, we must compare the GDP per capita of each African country covered by Starlink against the cheapest Starlink coverage option. Since GDP per capita reflects the country's average yearly income, Figure 9 displays the level of investment Starlink is for households in various countries. This final comparison reveals that Starlink's pricing is not focused on the average income of the population where they offer their service. Most importantly, it demonstrates that for the average person in some African countries, the initial cost of Starlink coverage is almost their entire yearly income. This observation suggests that despite Starlink's low average monthly broadband prices, factoring in their hardware expense is not economically feasible for some African countries.

Starlink's Impact on Local ISPs and Existing Initiatives

The demand for Starlink kits and the competition it has created in the telecommunications market has forced dominant African ISPs to respond by lowering their prices. An example of this can be seen with Safaricom, a telecommunications company (telco) with a significant market share in Kenya. In April 2023, Elon Musk stated his intention to enter the Kenyan Market, which led Safaricom to cut the cost of some Wi-Fi routers by half. When Starlink subsequently entered the market, they offered a 50 GB monthly data plan for Ksh1,300 ($10.16), which is more data and significantly cheaper than Safaricom's 45 GB plan for Ksh2,500 ($19.53). In September of 2024, Safaricom unveiled a new 1000Mbps (1 Gigabit per second) package in addition to increasing the speed of all of their lower speed packages, with their 40Mbps bundle now having its speed doubled to 80 Mbps.[34] This example illustrates two things: first, that competition between ISPs is great for consumers, and second, Starlink's entrance into the African market has created competition among ISPs.

This competition has led large ISPs in African countries to lobby their government to place new mandates and regulations on Starlink. Internet service providers in Kenya, Zimbabwe, Nigeria, and Cameroon have all raised concerns that Starlink is not being regulated fairly and suggest that they cannot compete with its services and pricing. In Kenya, a leaked letter Safaricom wrote to the Communication Authority of Kenya's director general suggested new regulations on Starlink. This letter stated that since satellites cover multiple countries, there can be unauthorised use, causing harmful interference in Kenya. Therefore, Safaricom argued that the Communications Authority of Kenya should require satellite

34 Safaricom, *Safaricom Increases Internet Speeds For Home And Business Customers, Introduces The New 1000Mbps Platinum Package For Customers*, 23 September 2024. Available at: https://www.safaricom.co.ke/media-center-landing/press-releases/safaricom-increases-internet-speeds-for-home-and-business-customers-introduces-the-new-1000mbps-platinum-package-for-customers (accessed: 30/10/2024); B. Okinda, Why Safaricom is panicking after Starlink's arrival in Kenya, *Afcacia*, 22 August 2024. Available at: https://afcacia.io/why-safaricom-is-panicking-after-starlinks-arrival-in-kenya/ (accessed: 30/10/2024).

providers to operate as "infrastructure providers" to operators like Safaricom.[35] With Starlink's *Direct to Cell* offering, this would not be the first time Starlink has partnered with operators as an infrastructure provider.[36] This regulation would importantly prevent Starlink from competing with Safaricom. Discussing competition in Kenya's telecommunications market, Kenyan President Ruto said that this competition makes all players better and has urged existing telcos to welcome new entrants.[37] This example illustrates Starlink's positive impact on affordability through the competition it offers but also reveals the enemies it is making within the African market that are wielding their influence against Starlink.

Starlink for Universal Meaningful Digital Connectivity

In their document outlining *Universal Meaningful Connectivity*, the ITU and OSET acknowledge that there cannot be a "one-size-fits-all policy mix that can be prescribed to all countries," alluding to their need to be open to all potential solutions.[38] Furthermore, in Resolution 71, titled *Strategic Plan for the Union for 2024–2027*, the ITU committed to working collaboratively with "the full range of other organisations and entities around the world committed to advancing the use of telecommunications/ICTs for a connected world by 2030."[39] This resolution reflects a commitment by the ITU to work with private companies that can help them achieve their target of universal, meaningful digital connectivity by 2030. To honour this commitment, the ITU has created the Partner2Connect initiative. This initiative comprises over four hundred fifty cross-sector entities that pledged to contribute over $50 billion towards global connectivity.[40] SpaceX is not included in this initiative.

---

35 A. Ross, Kenya's Safaricom urges new requirements for satellite providers like Starlink, *Reuters*, 23 August 2024. Available at: https://www.reuters.com/business/media-telecom/kenyas-safaricom-urges-new-requirements-satellite-providers-like-starlink-2024-08-23/ (accessed: 30/10/2024).

36 Starlink, *Specifications*; Starlink, *SpaceX Sends First Text Message Via Its Newly Launched Direct to Cell Satellites*, 10 January 2024. Available at: https://api.starlink.com/public-files/DIRECT_TO_CELL_FIRST_TEXT_UPDATE.pdf?_gl=1*1xtmfc*_ga*MTE1NDY0MDE4NC4xNzI2MDYyMzk0*_ga_S07SYD5D4F*MTczMDMwMTc4MC4xMi4wLjE3MzAzMDE3ODAuMC4wLjA. (accessed: 09/11/2024).

37 L. Yieke, Starlink's Aggressive Push in Africa Keeps Telcos on High Alert, *African Business*, 1 November 2024. Available at: https://african.business/2024/11/technology-information/starlinks-aggressive-push-in-africa-keeps-telcos-on-high-alert (accessed: 02/05/2025).

38 International Telecommunication Union & Office of the Secretary-General's Envoy on Technology, *op. cit.*, p. 4.

39 The Plenipotentiary Conference of the International Telecommunication Union, *Resolution 71: Strategic plan for the Union for 2024-–2027,* Bucharest 2022, p. 368. Available at: https://www.itu.int/en/council/Documents/basic-texts-2023/RES-071-E.pdf (accessed: 11/11/2024).

40 International Telecommunication Union*, ITU's Partner2Connect tops USD 50 billion for global connectivity at WSIS+20 Forum High Level Event: Digital Coalition surpasses half its USD 100 billion goal for closing the digital* divide, Geneva 2024. Available at: https://www.itu.int/en/mediacentre/Pages/PR-2024-05-27-Partner2Connect-global-connectivity.aspx (accessed: 11/11/2024).

Starlink's ability to provide 25–100 Mbps worldwide satisfies the ITU and OSET's infrastructure target and more than doubles their 10 Mbps speed target to qualify as meaningful connectivity. Within the document's *School Connectivity* connectivity enabler, the ITU and OSET set a target for all schools to obtain a minimum download speed of 20 Mbps by 2030. Starlink currently can exceed this ITU and OSET target. Furthermore, Starlink's *Direct to Cell* service would be able to exceed the ITU and OSET's stated target for its "Mobile network coverage" connectivity enabler.[41]

Therefore, according to the ITU and OSET's universal, meaningful connectivity document, Starlink is poised to satisfy three of eight infrastructure targets for 2030. Moreover, Starlink states on its website that there are numerous ways to procure equipment, including commercial and government channels. One then must ask: Why has Starlink not participated in multistakeholder initiatives led by the ITU or OSET?

One explanation could be competing geopolitical issues within international regulatory bodies, leading to gridlock. Starlink's violation of Iran's jurisdiction is an excellent example of how geopolitics is a significant obstacle preventing Starlink from cooperating with the ITU and OSET in their Universal Meaningful Connectivity targets for 2030. This case before the ITU Radio Regulations Board led to the decision requiring Starlink to cooperate with Iran to remove its hardware from the country.[42] This case, and Starlink's close cooperation with the US government in providing coverage to Iran, makes it hard for the ITU and OSET to collaborate with Starlink due to geopolitical tensions.

Comparative Analysis: Starlink vs. Other Satellite Broadband Companies

SpaceX's Starlink has achieved many important landmarks in the LEO satellite broadband market. Other LEO satellite Internet companies have significant differences. In their 2024 article detailing the competition in the LEO satellite Internet market, Pedram and Georgiades stated that Starlink, Project Kuiper, and OneWeb "are the salient projects in the LEO constellations industry".[43] Since OneWeb presents a much more significant divergence from Starlink and Kuiper's market

41 International Telecommunication Union & Office of the Secretary-General's Envoy on Technology, *op. cit.*, p. 4.

42 A. Akbari, Shutting down the internet is another brutal blow against women by the Iranian regime, *The Guardian*, 9 September 2022. Available at: https://www.theguardian.com/commentisfree/2022/sep/26/elon-musk-iran-women-mahsa-amini-feminists-morality-police (accessed: 04/11/2024); D. Psaledakis, S. Lewis, U.S. adjusts sanctions to help Iranians evade online surveillance, censorship, *Reuters*, 23 September 2022. Available at: https://www.reuters.com/world/us-expands-sanctions-exceptions-help-provide-internet-iranians-2022-09-23/ (accessed: 04/11/2024); International Telecommunication Union, *Document RRB24-2/12-E: Summary of decisions of the 96th meeting of the Radio Regulations Board*, Geneva 2024, pp. 13–15. Available at: https://www.itu.int/dms_pub/itu-r/md/24/rrb24.2/c/R24-RRB24.2-C-0012!!PDF-E.pdf (accessed: 11/11/2024).

43 M. Pedram, E. Georgiades, The Role of Regulatory Frameworks in Balancing Between National Security and Competition in LEO Satellite Market, *Journal of National Security Law & Policy*, 2024, 14(2), pp. 179–212.

strategies and is the only other functional LEO satellite internet constellation, this section will explore the differences between OneWeb and Starlink. This contrast will illuminate alternative strategies within the LEO satellite broadband industry. Additionally, it will provide parallels between the private and intergovernmental approaches to connecting the rest of the world to the Internet.

As of October 2024, OneWeb is the second-largest operational LEO constellation with over 600 satellites, working with a fleet of thirty-six GEO satellites. Initially created in 2012, OneWeb eventually filed for bankruptcy and was bought out in a joint purchase by the UK government and Indian conglomerate Bharti Global Ltd. in 2020. In 2023, Eutelsat, a French geostationary satellite business, merged with OneWeb to form the Eutelsat group, which became the first GEO-LEO integrated satellite group. The mission statement of this group states that they will "anticipate future needs with cutting-edge satellite technology, opening ways to new forms of communication which enable all to connect across the globe".[44] OneWeb is not owned by one company or individual.

The user hardware is separated into three offerings and differs based on its intended use. Among their offering are a foldable dish, a dish designed to be mounted on a car, and a large dish capable of connecting a small community to the Internet, offering speeds up to 195 Mbps.[45] Eutelsat Group's infrastructure connects businesses, ships, planes, existing telecom operators, governments, and organisations supporting universal service commitments. The group does not offer plans to individual users, a key difference from Starlink. This means that OneWeb does not directly compete with African telecommunications markets for users and functions more as an infrastructure provider.

Overlap and Differentiation

According to Pedram and Georgiades, the LEO satellite Internet market can be split into two stages. "Stage One" is described as the satellite launch phase. "Stage Two" is the satellite constellation signifying the LEO space that a company's satellites occupy and the capabilities of their satellites.[46] Within this division of the market, the authors warn about the creation of the vertical integration of these two stages that can then lead to companies being gatekeepers to the market. As gatekeepers, these companies could raise the entry price and subsequently reduce the

44 Eutelsat Group, *About. Eutelsat Group*, 2023. Available at: https://www.eutelsat.com/en/group/about-us.html#:~:text=OUR%20MISSION,-Enabling%20all%20to&text=Eutelsat%20Group%E2%80%99s%20mission%20is%20to,to%20connect%20across%20the%20globe (accessed: 11/11/2024). Eutelsat Group, *About \ Eutelsat Group*, Paris 2023. Available at: https://www.eutelsat.com/en/group/about-us.html#:~:text=OUR%20MISSION,-Enabling%20all%20to&text=Eutelsat%20Group%E2%80%99s%20mission%20is%20to,to%20connect%20across%20the%20globe (accessed: 11/11/2024).

45 Eutelsat OneWeb, *Carrier & Enterprise. World Leading Partners in User Terminal Technology*, Eutelsat Group, Paris 2024. Available at: https://oneweb.net/solutions/carrier-enterprise (accessed: 05/11/2024).

46 M. Pedram, E. Georgiades, *op. cit.*

competition. Therefore, this chapter's analysis of the overlap and differentiation of the two competitors will focus on their competencies in these two stages. By building upon the work of Pedram and Georgiades, this analysis reveals not only differences in market strategies but also Starlink's potential to become a gatekeeper that restricts competition.

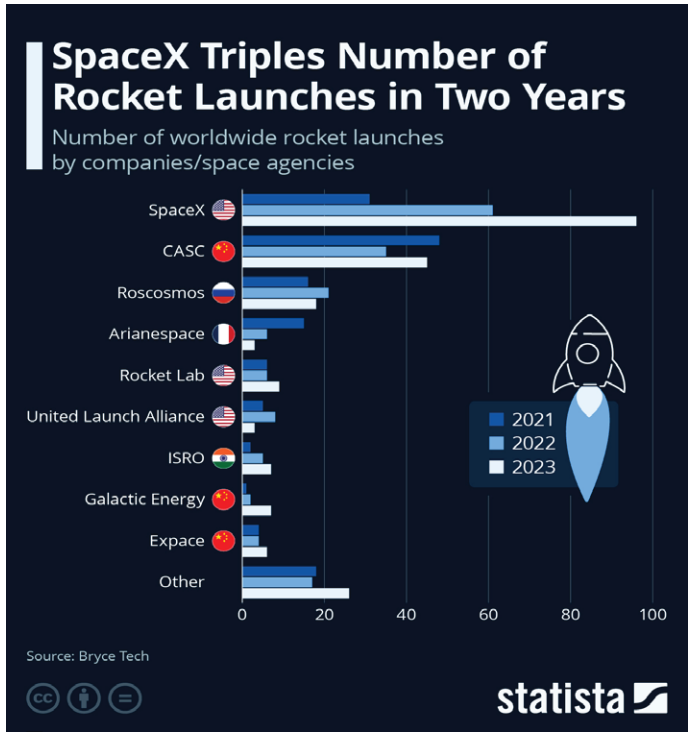


Figure 10. Number of Worldwide Rocket Launches by companies/space agencies
Source: F. Zandt, Infographic: SpaceX triples number of rocket launches in two years, *Statista*, 14 October 2024. Available at: https://www.statista.com/chart/29410/number-of-worldwide-rocket-launches-by-companies-and-space-agencies/ (accessed: 06/11/2024).

What can be ascertained from recent figures is that SpaceX has a dominant position over Stage One of the satellite broadband market. As illustrated in the figure above, SpaceX has facilitated over 50% of private launches in 2023.[47] SpaceX's success in this stage can be attributed to the affordability of its launches.[48]

47 F. Zandt, Infographic: SpaceX triples number of rocket launches in two years, *Statista*, 14 October 2024. Available at: https://www.statista.com/chart/29410/number-of-worldwide-rocket-launches-by-companies-and-space-agencies/ (accessed: 06/11/2024).

48 P. Lionnet, SpaceX and the categorical imperative to achieve low launch cost, *SpaceNews*, 7 June 2024. Available at: https://spacenews.com/spacex-and-the-categorical-imperative-to-achieve-low-launch-cost/ (accessed: 11/11/2024); D. Chow, To cheaply go: How falling launch

Whereas other space companies focus on saving money by cutting material or personnel costs, SpaceX has achieved its savings primarily through reusing the same rocket and integrating more robotics in production.[49] This capture of Stage One of the market has been critical in Starlink becoming the largest LEO constellation and enabled SpaceX to capture large swaths of the consumer base.

OneWeb, on the other hand, does not have its own launch service; instead, it has opted to launch its satellites with various actors, ranging from NewSpace India Limited to SpaceX. The diversity of partners OneWeb has integrated into its launches speaks towards its divergent path and collaborative nature.

Starlink has highly advanced satellites.[50] Quilty Space research analysts have stated that SpaceX has significantly improved its satellite's capacity to process and relay data in its new V2 satellite and projected more advancements in its V3.[51] Quilty Space research director Caleb Henry reportedly stated that their satellite mastery comes from its "aggressive vertical integration and high-volume production".[52] Henry noted that SpaceX can avoid many costs associated with external suppliers. This vertical integration also expresses Starlink's desire to control the "Stage Two" market.

According to its CEO, Eva Berneke, OneWeb's multi-orbit satellite infrastructure provides them with increased resiliency, which is particularly enticing for military and government users. Berneke included that the benefit lies in fitting a multi-network offering with a mobile backhaul on the go within a single piece of hardware that can fit into a tight space such as a plane.[53] The constellation is working to achieve 90% global connectivity by the end of 2024. OneWeb's divergence

---

costs fueled a thriving economy in orbit, *NBC News*, 4 April 2022. Available at: https://www.nbcnews.com/science/space/space-launch-costs-growing-business-industry-rcna23488 (accessed: 06/11/2024).

49 N. John, Raise the Space Bar: As SpaceX provides some of cheapest satellite launches, what can ISRO do to reclaim cost advantage?, *The Economic Times*, 3 November 2024. Available at: https://economictimes.indiatimes.com/news/science/raise-the-space-bar-as-spacex-provides-some-of-cheapest-satellite-launches-what-can-isro-do-to-reclaim-cost-advantage/articleshow/114889658.cms?from=mdr (accessed: 06/11/2024).

50 Starlink, *Satellite Technology*, 2024. Available at: https://www.starlink.com/technology (accessed: 11/11/2024).

51 S. Clark, SpaceX Pausing Launches of New-Generation Starlink Satellites, *Spaceflight Now*, 23 March 2023. Available at: https://spaceflightnow.com/2023/03/23/spacex-pausing-launches-of-new-generation-starlink-satellites (accessed: 11/11/2024).

52 S. Erwin, Starlink soars: SpaceX's satellite internet surprises analysts with $6.6 billion revenue projection, *SpaceNews*, 9 May 2024. Available at: https://spacenews.com/starlink-soars-spacexs-satellite-internet-surprises-analysts-with-6-6-billion-revenue-projection/ (accessed: 11/11/2024); *Starlink soars: SpaceX's satellite internet surprises analysts with $6.6 billion revenue projection*, SpaceNews, May 9, 2024. Available at: https://spacenews.com/starlink-soars-spacexs-satellite-internet-surprises-analysts-with-6-6-billion-revenue-projection/ (accessed: 11/11/2024).

53 J. Rainbow, Making the case for multi-orbit broadband, *SpaceNews*, 4 June 2024. Available at: https://spacenews.com/making-case-multi-orbit-broadband/ (accessed: 11/11/2024).

from Starlink's approach is also seen within this stage. Rather than focusing on vertical integration, the service provider has sold its stake in a satellite production facility and focused on collaboration. Eutelsat OneWeb is now looking for a manufacturer to build a second-generation LEO constellation to increase capacity and enhance the performance of their Gen 1.[54]

Policy and Regulatory Challenges in Africa

As explained in the sections above, Satellites provide Internet connectivity primarily through radio spectrum. However, radio spectrum is a limited resource. Entities that use this spectrum, such as ISPs, television stations, or radio stations, must be permitted to use it by each country where they wish to provide their service. Since multiple companies and industries need to use radio spectrum to operate, many existing companies and industries are hostile to Starlink and other LEO satellite broadband entry into the market. The ITU Radio Communication Sector (ITU-R) presides over international regulations and disputes. The ITU-R manages the spectrum coordination between countries to prevent interference, and countries authorise and license the spectrum allocation within their borders. Therefore, Starlink must obtain permission from each country to utilise the radio frequency within their borders.

Spectrum and Licensing Issues

At the World Communication Conference 2023 (WRC-23) held in Dubai, terrestrial telecommunications companies, GEO and GSO satellite-based companies, and LEO satellite broadband companies fought over international guidelines for spectrum allocation. On one side of the argument, GEO and GSO satellite-based companies claimed that LEO satellites caused interference. On the other side, LEO satellite broadband companies are pushing to update the rules to permit non-geostationary satellite systems (NGSO) to increase the equivalent power flux density (EPFD). EPFD measures a radio signal's power when it reaches Earth's surface. NGSO companies argue that current limits are outdated and are restricting the ability to make Internet access more affordable.[55] These arguments speak to strains placed upon regulatory bodies to determine what is best for various industries effectively.

54 J. Rainbow, Eutelsat scales back OneWeb Gen 2 upgrade plan, *SpaceNews*, 16 February 2024. Available at: https://spacenews.com/eutelsat-scales-back-oneweb-gen-2-upgrade-plan/ (accessed: 11/11/2024).

55 S. Dalledonne, *From WRC-23 to the next cycle: How to make everyone happy? (Hint: You can't)*, Policy Brief 66. European Space Policy Institute, 21 March 2024. Available at: https://www.espi.or.at/briefs/from-wrc-23-to-the-next-cycle-how-to-make-everyone-happy-hint-you-cant/ (accessed: 11/11/2024).

Geopolitics and sovereignty are also tied into the spectrum and licensing constraints. For example, the United States' National Spectrum Strategy states, "America's security, safety, technological leadership, and economic growth depend, in no small measure, on sufficient access to spectrum".[56] Starlink's illegal use in Iran illustrates the ability of private companies to disregard independent states' spectrum rights, but most importantly, their ability to influence the flow of information within and outside of its borders. Another important connection is to Internet shutdowns. According to AccessNow, in 2023, there were 283 Internet shutdowns in 39 countries, the highest since they began monitoring in 2016, with many of these being African countries.[57] The report indicates how Internet shutdowns are a tool increasingly being deployed by many African countries that desire to have control over information flow from within and outside of their country.

Public-Private Partnerships

There have been multiple instances where private companies have partnered with LEO satellite broadband. Africa's leading digital and infrastructure service provider, Bayobab, has agreed to work with OneWeb to help deliver fixed connectivity services and improve coverage of rural areas throughout Africa.[58] Additionally, OneWeb signed an agreement with Airtel Africa to achieve full coverage across all of Airtel Africa's markets, which includes fourteen African countries. Subsequently, in August of 2024, Airtel Nigeria announced the successful installation of a OneWeb dish at a site in Lagos, stating that it would help governments and businesses connect rural areas.[59] Within the "Overlap and Differentiation" section above, it was established that OneWeb's market strategy diverged significantly from Starlink. This section represents a continued focus from OneWeb on prioritising collaboration and partnerships with outside businesses and industries.

Starlink is also actively working with other providers to assist rural communities in connecting to the Internet. It should be noted that Starlink has just introduced its "Community Gateways" package for local providers. This package offers up to 10 Gigabits per second (Gbps) of download and 10 Gbps of upload with less than 99 milliseconds of latency. By utilising last-mile fibre, fixed wireless and mobile wireless providers

56 The White House, *The National Spectrum Strategy*, 13 Nov. 13,ember 2023, pp. 9–10. Available at: https://www.ntia.gov/sites/default/files/publications/national_spectrum_strategy_final.pdf (accessed: 11/11/2024).

57 Z. Rosson, C. Tackett, Felicia, The Most Violent Year: Internet Shutdowns in 2023, *Access Now*. Available at: https://www.accessnow.org/internet-shutdowns-2023/ (accessed: 06/11/2024).

58 Bayobab, *Eutelsat and Bayobab Collaborate on OneWeb Constellation for Fixed Services throughout Africa*, 23 August 2024. Available at: https://bayobab.africa/eutelsat-and-bayobab-collaborate-on-oneweb-constellation-for-fixed-services-throughout-africa/ (accessed: 05/11/2024).

59 S. Nyangi, Airtel Nigeria Successfully Installs Eutelsat OneWeb Dish, *Space in Africa*, 23 August 2024. Available at: https://spaceinafrica.com/2024/08/23/airtel-nigeria-successfully-installs-eutelsat-oneweb-dish/ (accessed: 05/11/2024).

would be given enough throughput to serve thousands of new customers.[60] This option is tailored to work for hard-to-reach communities such as the ones in Africa. Yet, it costs $75,000 per Gbps monthly and $1.25 million upfront, which might not be feasible for some existing African telecommunications companies.

Case Studies: Early Starlink Deployment in Africa

For years, experts have recognised Africa's development potential and claimed it to be the fastest-growing consumer market in the world.[61] Starlink's arrival on the continent has elicited strong pushback from many countries and telecommunications companies. Oniosun, the CEO of a Nigerian media and analytics company focused on the African space and satellite industry, stated: "We have a foreign company coming in, doing the bare minimum, and then taking market share from companies that have invested heavily in the continent and are providing jobs for thousands of people".[62]

Others, such as Kenyan President Ruto, say that this competition makes all players better and has urged existing telcos to welcome new entrants. Furthermore, industry operators, such as South Africa's MTN Group, see Starlink as an opportunity to allow for higher digital penetration rates.[63] Therefore, in this section, we will explore Starlink's impact through its coverage in Nigeria and its challenges in offering coverage in South Africa.

South Africa

The birthplace of SpaceX founder Elon Musk and the most advanced economy in the continent, South Africa, is a focus for Starlink's coverage expansion. Independent Communications Authority of South Africa (ICASA), the body responsible for assigning the country's spectrum, banned Starlink from operating in South Africa. This ban is based on South Africa's Electronic Communications Act, which requires spectrum

60 P. Lipscomb, Starlink Unveils Community Gateway Offering Aimed at Plugging Coverage in Remote Areas, *Data Centre Dynamics*, 18 January 2024. Available at: https://www.datacenterdynamics.com/en/news/starlink-unveils-community-gateway-offering-aimed-at-plugging-coverage-in-remote-areas/ (accessed: 11/11/2024).

61 L. Signé, Africa's Consumer Market Potential, *Brookings*, 12 December 2018. Available at: https://www.brookings.edu/articles/africas-consumer-market-potential/ (accessed: 07/11/2024); African Development Bank Group, Africa Dominates List of the World's 20 Fastest-Growing Economies in 2024—African Development Bank Says in Macroeconomic Report. *Press Release*, African Development Bank Group. 16 February 2024. Available at: https://www.afdb.org/en/news-and-events/press-releases/africa-dominates-list-worlds-20-fastest-growing-economies-2024-african-development-bank-says-macroeconomic-report-68751 (accessed: 07/11/2024).

62 L. Yieke, *Starlink's* Aggressive Push in Africa Keeps Telcos on High Alert, *African Business*, Nov. 1, 2024. Available at: https://african.business/2024/11/technology-information/starlinks-aggressive-push-in-africa-keeps-telcos-on-high-alert (accessed: 11/11/2024).

63 *Ibidem*.

licensees to have 30% equity ownership by persons from historically disadvantaged groups.[64] Starlink's refusal to abide by this regulation is consistent across numerous African countries. Kenya and Zimbabwe have this same law, but Starlink made deals with the countries' leaders to have SpaceX forgo this regulation. This provides more context to Kenyan ISP Safaricom's claims that Starlink is being regulated unfairly.[65]

One ICASA councillor, Charley Lewis, believes satellite broadband connectivity is not the solution to the digital divide. Lewis stated that equipment and monthly service costs put it "out of the reach of poor individuals".[66] Despite its being illegal, South Africans still bought Starlink hardware and utilised its roaming capabilities. Through this process, thousands of users in South Africa could use the service without official government authorisation. On October 25, 2024, Starlink users in South Africa noticed that Starlink removed its roaming subscription options.[67] South African President Ramaphosa talked with Elon Musk at a UN General Assembly, where he told him, "I want you to come home and invest here".[68] South Africa's Minister of the Department of Communications and Digital Technologies (DCDT), Solly Malasti, then announced his intentions to amend the Electronic Communications Act. Malasti stated he wanted to "significantly expand access to broadband connectivity to poor South Africans and people living in remote parts of the country".[69] Powerful South African officials, such as Malasti and Ramaphosa, are therefore willing to adjust their regulatory policy on the radio spectrum to accommodate Starlink and similar companies. This speaks to a position of leverage that Starlink, and potentially other LEO satellite operators, have, and in Starlink's case, is exercising over African countries. Additionally, it provides some credence to claims made by African ISPs explored in this chapter's case study analysis of Safaricom.

Nigeria

Nigeria is the most populous nation within the continent and was the first African country to sign a spectrum licensing agreement with Starlink in January of

64 M. Akuchie, South African authorities ban importation of Starlink kits as users face possible blackout, *Technext*, 22 August 2023. Available at: https://technext24.com/2023/08/22/sa-starlink-ban-kits-import/ (accessed: 11/11/2024).

65 A. Ross, *op. cit*.

66 S. Quadri, Elon Musk's Starlink shakes up competition in Africa, *Semafor*, 23 September 2024. Available at: https://www.semafor.com/article/09/23/2024/elon-musks-starlink-shakes-up-competition-in-africa (accessed: 14/10/2024).

67 H. Labuschagne, Starlink says South Africa will be a top 10 country for its service, *MyBroadband*, 25 October 2024. Available at: https://mybroadband.co.za/news/broadband/566758-starlink-says-south-africa-will-be-a-top-10-country-for-its-service.html (accessed: 11/11/2024).

68 L. Yieke, Starlink's Aggressive Push in Africa Keeps Telcos on High Alert, *African Business*, 1 November 2024. Available at: https://african.business/2024/11/technology-information/starlinks-aggressive-push-in-africa-keeps-telcos-on-high-alert (accessed: 11/11/2024).

69 M. Sehloho, South Africa could amend law blocking Starlink entry, *Connecting Africa*, 8 October 2024. Available at: https://www.connectingafrica.com/regulation/south-africa-could-amend-law-blocking-starlink-entry (accessed: 11/11/2024).

2023.[70] Since 2023, Starlink has become the third-largest ISP in Nigeria by subscriber count.[71] Moreover, Starlink has been actively working to make the service more affordable and connect rural and hard-to-reach regions in the country. After signing a deal with Starlink, Africa Mobile Networks (AMN) could use Starlink terminals for low-latency satellite backhaul to its multi-carrier radio access node, the ARN. With this deal, AMN can accommodate large data volumes and ensure affordability. AMN reported a 45% increase in Internet traffic across its 100 rural base stations following this implementation.[72] Additionally, Starlink is facing such a high demand in big African cities that they had to halt new subscribers in dense cities to adjust to the high demand, impacting five cities in Nigeria alone.[73] This shows that Starlink is being used in certain areas to address the two most significant barriers to connectivity in Africa, which are affordability and coverage, as revealed in this chapter's introduction.

Starlink's success in Nigeria has drawn the ire of many who argue that the NCC should utilise its regulatory capacity to even the playing field. Leaders of African ISPs, such as eStream Network CEO Muyiwa Ogungboye, have expressed frustration with the NCC's lack of recognition of the investments already made by Indigenous people in ICT infrastructure. Gbolahan Awonuga, the head of operations at the Association of Licensed Telecoms Operators of Nigeria (ALTON), has gone further, stating that Starlink might lead to the extinction of ISPs.[74] Even the head of a Nigerian pan-African digital inclusion NGO, Gbenga Sesan, argues that achieving universal coverage through Starlink is not the best use of the country's collective resources. Sesan explained that Nigerians could use their collective resources to help establish terrestrial connectivity through the numerous subsea cable landing points in the country.[75] Therefore, NGOs and telcos in Nigeria have expressed concern about relying on foreign companies to supply critical infrastructure.

In October 2024, The Nigerian Communication Commission commenced "pre-enforcement action" against Starlink for its 97% price hike to their standard service subscription that Starlink stated was due to high inflation. According to the NCC, Starlink violated sections 108 and 111 of the Nigerian Communications Act in conducting this high price increase without the NCC's approval. These sections specifically relate to the protection of consumers and the requirement

70 A. Onukwue, Starlink puts halt on new customers in Africa, *Semafor*, 5 November 2024. Available at: https://www.semafor.com/article/11/05/2024/elon-musk-starlink-halts-africa-customer-sign-ups (accessed: 11/11/2024).

71 Nigerian Communications Commission, *Internet Service Operator Data: Quarter 4-2023*, 2024. Available at: https://www.ncc.gov.ng/statistics-reports/subscriber-data#internet-service-operator-data (accessed: 09/11/2024).

72 S. Nyangi, *op. cit.*

73 Starlink, *Availability Map*.

74 J. Adejumoh, More Troubles for Telcos, ISPs As Starlink Deepens Operations in Nigeria, *Independent*, 26 August 2024. Available at: https://independent.ng/more-troubles-for-telcos-isps-as-starlink-deepens-operations-in-nigeria/ (accessed: 11/11/2024).

75 S. Quadri, *op. cit.*

of the licensee to provide information to the NCC that justifies their rate increase so the NCC can assess whether the adjustments are justifiable.[76] Since this time, Starlink has claimed to reverse the price hike; yet, according to The Guardian, sources stated that the NCC would serve a query to Starlink to ask the company why the NCC should not take disciplinary action. The source further noted that "the sanction is needed to set the record straight and ensure licensees in the sector don't flout regulatory orders".[77] This act illustrates not only the power governments can hold over satellite broadband operators such as Starlink but also the first time any country's communications authority has taken such action. Therefore, the Nigerian Communication Commission has become an early indicator of how Starlink will navigate these regulations and be a worldwide blueprint for spectrum regulatory bodies.

Lessons from Early Developments

We can conclude from these two case studies that Starlink has gained a large following in Africa and has experienced immense growth in subscribers. These case studies also illustrate Starlink's strategy and proven ability to have countries adapt their policy around the company's aims. This strategy also provides some credence to the complaints of some African ISPs claiming Starlink is being regulated unfairly.[78] The decision of the Nigerian Communication Commission to take action against Starlink's price hikes might lead to a shift in countries' regulatory approach to Starlink and other LEO satellite ISPs. Starlink's ability to drastically increase Internet penetration, make connectivity more affordable, and deliver high-speed Internet to rural areas is undeniable and widely recognised. By focusing on the regulatory barriers to Starlink's expansion, this case study reveals that a lack of collaboration with countries' regulations may create space for more collaborative competitors.

Future Prospects and Conclusion

Groundbreaking developments led by SpaceX through their Starlink LEO satellite constellation have made it possible to achieve the goals of many connectivity initiatives in a time frame that would have been significantly prolonged with terrestrial infrastructure. Several roadblocks still stand in the way of attaining historic goals set in place over decades ago. However, Starlink's close association with the United States is a geopolitical roadblock that it may never overcome in some countries.

76 M. Iderawumi, NCC initiates pre-enforcement action against Starlink over price hike, *Space in Africa*, 8 October 2024. Available at: https://spaceinafrica.com/2024/10/08/nigerian-communications-commission-responds-to-starlinks-unapproved-price-hike/ (accessed: 07/11/2024).

77 A. Adepetun, NCC may sanction Starlink over price hike, despite reversal, *The Guardian*, 28 October 2024. Available at: https://guardian.ng/news/ncc-may-sanction-starlink-over-price-hike-despite-reversal/ (accessed: 11/11/2024).

78 A. Ross, *op. cit.*

The importance of a country's ability to control the flow of information within its borders will continue to grow. The significance placed on the ability to control the flow of information might cause some African countries to prefer terrestrial connectivity methods.

Incumbent telecommunications companies and ISPs within Africa have voiced considerable opposition to the entrance of Starlink into their market. While such a reaction is expected, the opposition from NGOs signals potential challenges for Starlink's future. A coalition of local telcos and NGOs lobbying against Starlink and other LEO satellite operators could wield significant influence to block Starlink from entering new markets. Therefore, LEO satellite operators in Africa that prioritise collaboration with local ISPs to create affordable connectivity solutions seem to be the best long-term strategy for connecting most of the African market. If executed properly, this collaborative approach diminishes the chances of local telcos and NGOs lobbying against the company's operation since everyone stands to benefit from the arrangement. African telcos, such as Safaricom, are already pushing for these collaborations, and by building up local ICT infrastructure and providing more local jobs, they would be addressing concerns voiced by advocates and NGOs.[79] Effective cooperation between actors in the African telecommunications market would lead to a mutually beneficial arrangement that benefits all actors.

The potential of LEO satellite broadband technology is evident and provides Starlink with its current position of leverage in negotiations with countries over spectrum allocation. Regulatory bodies are still adjusting to LEO satellite broadband's entrance into the market. Therefore, if regulatory agencies in African countries exercise their control over radio spectrum allocation to Starlink more strictly, which is currently playing out in Nigeria, it may present a chance for Starlink's more collaborative competitors to gain a stronger foothold in the market.

SpaceX's achievements through Starlink have changed the global ICT landscape forever, but perhaps most so in Africa, where Internet penetration and affordability are the lowest.[80] Starlink's ability to provide global coverage and competition to the ICT market is evident and widely discussed. The evolving regulatory environment can drastically change market positions. OneWeb has taken a divergent approach from its competitor, Starlink, and has opted for more collaborative development in its launch and satellite services. Given the intense backlash Starlink has experienced from African ISPs and NGOs and their collective ability to impact regulatory bodies, a collaborative approach may be the best long-term strategy. Therefore, the domestic regulatory responses, especially those related to spectrum policies, are key considerations when addressing how Starlink has impacted connectivity initiatives in Africa.

79 *Ibidem*.

80 International Telecommunication Union, *Facts and figures 2023 – Internet use in urban and rural areas*, 2024. Available at: https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use-in-urban-and-rural-areas (accessed: 30/09/2024); International Telecommunication Union, *Statistics*; M. Shanahan, K. Bahla, *op. cit.*

Whether Starlink fits within the mould of a private connectivity initiative like 2Africa or one led by an intragovernmental organisation with a global vision reveals Starlink's singularity. Starlink's goal to provide Internet coverage for the whole world and openness suggests it is similar to the UN's initiative. Yet, Starlink's ability to work around regulations in some African countries resembles the 2Africa example of the private connectivity initiative. Due to the geopolitical nature of space and the importance of Internet infrastructure, Starlink is the nexus of technologies of great interest to individual states. LEO satellite ISPs have the capacity to amplify the ability to control global information to the whole world rather than within one country. Starlink's close cooperation with the United States in its foreign policy objectives indicates the power of this technology. Therefore, Starlink is paving the way for a new type of global connectivity initiative backed by individual states and utilised to fulfill the geopolitical aims of that particular state. Ultimately, when comparing this current state of satellite broadband to the aims of the ITSO established by the Tunis Agenda, it reveals Starlink's most significant impact on the shifting telecommunications market.

Bibliography

2Africa, About. 2Africa Cable2Africa Deployment Is Underway. 2Africa Is Now Landing across 3 Continents and Will Be Ready for Service in Most Places as Early as 2023, *2Africa Cable*, 2022. Available at: https://www.2africacable.net/about (accessed: 02/02/2025).

Adejumoh, J., More Troubles for Telcos, ISPs As Starlink Deepens Operations in Nigeria, *Independent*, 26 August 2024. Available at: https://independent.ng/more-troubles-for-telcos-isps-as-starlink-deepens-operations-in-nigeria/ (accessed: 11/11/2024).

Adepetun, A., NCC may sanction Starlink over price hike, despite reversal, *The Guardian*, 28 October 2024. Available at: https://guardian.ng/news/ncc-may-sanction-starlink-over-price-hike-despite-reversal/ (accessed: 11/11/2024).

African Development Bank Group, Africa Dominates List of the World's 20 Fastest-Growing Economies in 2024—African Development Bank Says in Macroeconomic Report, *Press Release*, African Development Bank Group. 16 February 2024. Available at: https://www.afdb.org/en/news-and-events/press-releases/africa-dominates-list-worlds-20-fastest-growing-economies-2024-african-development-bank-says-macroeconomic-report-68751 (accessed: 07/11/2024).

African Union, *The Digital Transformation Strategy For Africa (2020–2030)*, Addis Ababa, African Union, Ethiopia 2020. Available at: https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

Akbari, A., Shutting down the internet is another brutal blow against women by the Iranian regime, *The Guardian*, 9 September 2022. Available at: https://www.theguardian.com/commentisfree/2022/sep/26/elon-musk-iran-women-mahsa-amini-feminists-morality-police (accessed: 04/11/2024).

Akcali Gur, B., **Kulesza, J.**, Equitable Access to Satellite Broadband Services: Challenges and Opportunities for Developing Countries, *Telecommunications Policy*, 2024, 48(5), pp. 1–10, https://doi.org/10.1016/j.telpol.2024.102731

Akuchie, M., South African authorities ban importation of Starlink kits as users face possible blackout, *Technext*, 22 August 2023. Available at: https://technext24.com/2023/08/22/sa-starlink-ban-kits-import/ (accessed: 11/11/2024).

Association for Progressive Communication, IT for Change, and WACC Global and Swedish International Development Cooperation Agency, Special Edition: WSIS+20: Reimagining Horizons of Dignity, Equity and Justice for Our Digital Future, *Global Information Society Watch*, 2024. Available at: https://www.giswatch.org/2024-special-edition-wsis20-reimagining-horizons-dignity-equity-and-justice-our-digital-future (accessed: 05/11/2024).

Bayobab, *Eutelsat and Bayobab Collaborate on OneWeb Constellation for Fixed Services throughout Africa*, 23 August 2024. Available at: https://bayobab.africa/eutelsat-and-bayobab-collaborate-on-oneweb-constellation-for-fixed-services-throughout-africa/ (accessed: 05/11/2024).

Bennett, M., **Kramer, C.**, *Large Constellations of Low-Altitude Satellites: A Primer*, Congressional Budget Office, 2023. Available at: https://www.cbo.gov/publication/58794 (accessed: 02/05/2025).

Capannolo, A., **Silvestrini, S.**, **Colagrossi, A.**, **Pesce, V.**, *Chapter Four—Orbital Dynamics*, [in:] V. Pesce, A. Colagrossi, S. Silvestrini (eds.), *Modern Spacecraft Guidance, Navigation, and Control*, Elsevier, 2023, pp. 131–206, https://doi.org/10.1016/B978-0-323-90916-7.00004-4

Chair, C., Internet Use Barriers And User Strategies: Perspectives from Kenya, Nigeria, South Africa and Rwanda, *Research ICT Africa, Beyond Access Policy Paper*, 2017, 1, pp. 1–42.

Chow, D., To cheaply go: How falling launch costs fueled a thriving economy in orbit, *NBC News*, 4 April 2022. Available at: https://www.nbcnews.com/science/space/space-launch-costs-growing-business-industry-rcna23488 (accessed: 06/11/2024).

Clark, S., SpaceX Pausing Launches of New-Generation Starlink Satellites, *Spaceflight Now*, 23 March 2023. Available at: https://spaceflightnow.com/2023/03/23/spacex-pausing-launches-of-new-generation-starlink-satellites (accessed: 11/11/2024).

Communications Authority of Kenya, Fourth quarter sector statistics report for the financial year 2023/2024 (1st April–30th June 2024), *Communications Authority of Kenya*, 2024. Available at: https://www.ca.go.ke/sites/default/files/2024-10/Sector%20Statistics%20Report%20Q4%202023-2024.pdf

Dalledonne, S., *From WRC-23 to the next cycle: How to make everyone happy? (Hint: You can't)*, Policy Brief 66. European Space Policy Institute, 21 March 2024. Available at: https://www.espi.or.at/briefs/from-wrc-23-to-the-next-cycle-how-to-make-everyone-happy-hint-you-cant/ (accessed: 11/11/2024).

DeGrasse, M., Amazon exec Dave Limp unveils Project Kuiper user terminals. Satellite 2023 show daily—Day 3, *Via Satellite*, 14 March 2023. Available at: https://interactive.satellitetoday.com/via/satellite-2023-show-daily-day-3/amazon-exec-dave-limp-unveils-project-kuiper-user-terminals

Erwin, S., Starlink soars: SpaceX's satellite internet surprises analysts with $6.6 billion revenue projection, *SpaceNews*, 9 May 2024. Available at: https://spacenews.com/starlink-soars-spacexs-satellite-internet-surprises-analysts-with-6-6-billion-revenue-projection/ (accessed: 11/11/2024).

Eutelsat Group, *About. Eutelsat Group*, 2023. Available at: https://www.eutelsat.com/en/group/about-us.html#:~:text=OUR%20MISSION,-Enabling%20all%20to&text=Eutelsat%20Group%E2%80%99s%20mission%20is%20to,to%20connect%20across%20the%20globe (accessed: 11/11/2024).

Eutelsat OneWeb, *Carrier & Enterprise. World Leading Partners in User Terminal Technology*, Eutelsat Group, Paris 2024. Available at: https://oneweb.net/solutions/carrier-enterprise (accessed: 05/11/2024).

Evans, J.V., The Proposed Ku-Band Non Geostationary Communication Satellite Systems, *Space an Integral Part of the Information Age*, 2000, 47(2), pp. 171–182, https://doi.org/10.1016/S0094-5765(00)00057-6

Hill, J., OneWeb's new military and emergency response terminal can fit inside a backpack, *Via Satellite*, 11 September 2023. Available at: https://www.satellitetoday.com/technology/2023/09/11/onewebs-new-military-and-emergency-response-terminal-can-fit-inside-a-backpack/

Holker, M., *27—Radiowave propagation*, [in:] F. Mazda (ed.), *Telecommunications engineer's reference book*, 1993, pp. 27–1, https://doi.org/10.1016/B978-0-7506-1162-6.50033-2

Howdle, D., Global Broadband Pricing League Table 2024, *Cable.co.uk*, 30 June 2024. Available at: https://www.cable.co.uk/broadband/pricing/worldwide-comparison/#regions (accessed: 30/10/2024).

Human Rights Council, *Resolution A/HRC/32/L.20: Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development*, 2016. Available at: https://www.article19.org/data/files/Internet_Statement_Adopted.pdf

Iderawumi, M., NCC initiates pre-enforcement action against Starlink over price hike, *Space in Africa*, 8 October 2024. Available at: https://spaceinafrica.com/2024/10/08/nigerian-communications-commission-responds-to-starlinks-unapproved-price-hike/ (accessed: 07/11/2024).

Imoisili Onuwabhagbe, G., **Kadiri, F.**, **Olawale, T.G.**, **Akinjobi, T.M.**, Internet access commercialization viability in Federal Polytechnic Offa using Starlink satellite connectivity, *International Journal of Advances in Engineering and Management (IJAEM)*, 2024, 6(08), pp. 232–237.

International Monetary Fund, *World economic outlook (October 2024) – GDP per capita, current prices*, 2024. Available at: https://www.imf.org/external/datamapper/NGDPDPC@WEO (accessed: 27/10/2024).

International Telecommunication Union & **Office of the Secretary-General's Envoy on Technology**, *Achieving universal and meaningful digital connectivity: Setting a baseline and targets for 2030*, United Nations, 2021. Available at: https://www.itu.int/itu-d/meetings/statistics/wp-content/uploads/sites/8/2022/04/UniversalMeaningfulDigitalConnectivityTargets2030_BackgroundPaper.pdf (accessed: 02/02/2025).

International Telecommunication Union, *Document RRB24-2/12-E: Summary of decisions of the 96th meeting of the Radio Regulations Board*, Geneva 2024, pp. 13–15. Available at: https://www.itu.int/dms_pub/itu-r/md/24/rrb24.2/c/R24-RRB24.2-C-0012!!PDF-E.pdf (accessed: 11/11/2024).

International Telecommunication Union, *Facts and figures 2023 – Internet use in urban and rural areas*, 2024. Available at: https://www.itu.int/itu-d/reports/statistics/2023/10/10/ff23-internet-use-in-urban-and-rural-areas (accessed: 30/9/2024).

International Telecommunication Union, *ITU's Partner2Connect tops USD 50 billion for global connectivity at WSIS+20 Forum High Level Event*, Geneva 2024. Available at: https://www.itu.int/en/mediacentre/Pages/PR-2024-05-27-Partner2Connect-global-connectivity.aspx

International Telecommunication Union, *Population of global offline continues steady decline to 2.6 billion people in 2023*, 2024. Available at: https://www.itu.int/en/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx (accessed: 02/02/2025).

International Telecommunication Union, *Statistics*, 2024. Available at: https://www.itu.int/en/ITU-D/Statistics/pages/stat/default.aspx (accessed: 21/10/2024).

International Telecommunication Union, *The pandemic has slowed wireless network buildouts: The FCC has granted some deadline extensions, but not as much as one industry group originally asked for*. *IEEE Spectrum*, 2020. Available at: https://spectrum.ieee.org/the-pandemic-has-slowed-wireless-network-buildouts

Internet Governance Forum, *WSIS+20 and IGF+20 review by the UN General Assembly (2025)*, 2024. Available at: https://www.intgovforum.org/en/content/wsis20-and-igf20-review-by-the-un-general-assembly-2025

Jewett, R., Amazon and Think Tanks Launch Group Advocating for Power Flux Density Changes, *Via Satellite*, 2023. Available at: https://www.satellitetoday.com/technology/2023/10/31/amazon-and-think-tanks-launch-group-advocating-for-power-flux-density-changes/

John, N., Raise the Space Bar: As SpaceX provides some of cheapest satellite launches, what can ISRO do to reclaim cost advantage?, *The Economic Times*, 3 November 2024. Available at: https://economictimes.indiatimes.com/news/science/raise-the-space-bar-as-spacex-provides-some-of-cheapest-satellite-launches-what-can-isro-do-to-reclaim-cost-advantage/articleshow/114889658.cms?-from=mdr (accessed: 06/11/2024).

Katkin, K., The global broadband satellite infrastructure initiative, *SSRN*, 2006, pp. 1–49. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2103932 (accessed: 02/02/2025).

Koziol, M., *Amazon's Project Kuiper is more than the company's response to SpaceX*, IEEE Spectrum, 2020. Available at: https://spectrum.ieee.org/amazons-project-kuiper-is-more-than-the-companys-response-to-spacex

Kumar, S., *The digital frontier*, Indiana University Press, 2021, https://doi.org/10.2307/j.ctv21hrjv1

Labuschagne, H., Starlink says South Africa will be a top 10 country for its service, *MyBroadband*, 25 October 2024. Available at: https://mybroadband.co.za/news/broadband/566758-starlink-says-south-africa-will-be-a-top-10-country-for-its-service.html (accessed: 11/11/2024).

Lionnet, P., SpaceX and the categorical imperative to achieve low launch cost, *SpaceNews*, 7 June 2024. Available at: https://spacenews.com/spacex-and-the-categorical-imperative-to-achieve-low-launch-cost/ (accessed: 11/11/2024).

Lipscomb, P., Starlink Unveils Community Gateway Offering Aimed at Plugging Coverage in Remote Areas, *Data Centre Dynamics*, 18 January 2024. Available at: https://www.datacenterdynamics.com/en/news/starlink-unveils-community-gateway-offering-aimed-at-plugging-coverage-in-remote-areas/ (accessed: 11/11/2024).

Liu, S., Gao, Z., **Wu, Y.**, **Ng, D.W.K.**, **Gao, X.**, **Wong, K.-K.**, **Chatzinotas, S.**, **Ottersten, B.**, LEO satellite constellations for 5G and beyond: How will they reshape vertical domains? *IEEE Communications Magazine*, 2021, 59(7), pp. 30–36, https://doi.org/10.1109/MCOM.001.2001081

McDowell, J., *Jonathan's Space Pages: Starlink Statistics – Starlink Launch Statistics*. Available at: https://planet4589.org/space/con/star/stats.html (accessed: 24/10/2024).

Mwema, E., Birhane, A., Undersea Cables in Africa: The New Frontiers of Digital Colonialism, *First Monday*, 2024, 29(4), pp. 1–28.

NASA Ames Research Center, Small Spacecraft Systems Virtual Institute, *State-of-the-art of small spacecraft technology*, National Aeronautics and Space Administration, 2024. Available at: https://www.nasa.gov/wp-content/uploads/2024/03/soa-2023.pdf (accessed: 24/10/2024).

Nchake, M.A., **Shuaibu, M.**, Investment in ICT infrastructure and inclusive growth in Africa, *Scientific African*, 2022, 17, e01293, https://doi.org/10.1016/j.sciaf.2022.e01293

Nigerian Communications Commission, *Internet service operator data: Quarter 4-2023*, 2024. Available at: https://ncc.gov.ng/market-data-reports/subscriber-statistics#internet-service-operator-data (accessed: 09/11/2024).

Nothias, T., Access granted: Facebook's Free Basics in Africa, *Media, Culture & Society*, 2020, 42(3), pp. 329–348, https://doi.org/10.1177/0163443719890530

Nyangi, S., Airtel Nigeria Successfully Installs Eutelsat OneWeb Dish, *Space in Africa*, 23 August 2024. Available at: https://spaceinafrica.com/2024/08/23/airtel-nigeria-successfully-installs-eutelsat-oneweb-dish/ (accessed: 05/11/2024).

Okinda, B., Why Safaricom is panicking after Starlink's arrival in Kenya, *Afcacia*, 22 August 2024. Available at: https://afcacia.io/why-safaricom-is-panicking-after-starlinks-arrival-in-kenya/ (accessed: 30/10/2024).

Onukwue, A., Starlink puts halt on new customers in Africa, *Semafor*, 5 November 2024. Available at: https://www.semafor.com/article/11/05/2024/elon-musk-starlink-halts-africa-customer-sign-ups (accessed: 11/11/2024).

Orgad, L., *Cloud communities: The dawn of global citizenship?*, [in:] R. Bauböck (ed.), *Debating Transformations of National Citizenship*, Cham: Springer International Publishing, 2018, pp. 251–260, https://doi.org/10.1007/978-3-319-92719-0_46

Pedram, M., Georgiades, E., The role of regulatory frameworks in balancing between national security and competition in LEO satellite market, *Journal of National Security Law & Policy*, 2024, 14(2), pp. 179–212.

The Plenipotentiary Conference of the International Telecommunication Union, *Resolution 71 (rev. Bucharest, 2022): Strategic plan for the union for 2024–2027*, Bucharest 2022. Available at: https://www.itu.int/en/council/Documents/basic-texts-2023/RES-071-E.pdf (accessed: 24/10/2024).

Pratt, S.R., Raines, R.A., Fossa, C.E., Temple, M.A., An operational and performance overview of the IRIDIUM low earth orbit satellite system, *IEEE Communications Surveys*, 1999, 2(2), pp. 2–10, https://doi.org/10.1109/COMST.1999.5340513

Psaledakis, D., Lewis, S., U.S. adjusts sanctions to help Iranians evade online surveillance, censorship, *Reuters*, 23 September 2022. Available at: https://www.reuters.com/world/us-expands-sanctions-exceptions-help-provide-internet-iranians-2022-09-23/ (accessed: 04/11/2024).

Quadri, S., Elon Musk's Starlink shakes up competition in Africa, *Semafor*, 23 September 2024. Available at: https://www.semafor.com/article/09/23/2024/elon-musks-starlink-shakes-up-competition-in-africa (accessed: 14/10/2024).

Rainbow, J., Eutelsat scales back OneWeb Gen 2 upgrade plan, *SpaceNews*, 16 February 2024. Available at: https://spacenews.com/eutelsat-scales-back-oneweb-gen-2-upgrade-plan/ (accessed: 11/11/2024).

Rainbow, J., Making the case for multi-orbit broadband, *SpaceNews*, 4 June 2024. Available at: https://spacenews.com/making-case-multi-orbit-broadband/ (accessed: 11/11/2024).

Riebeek, H., *Catalog of Earth Satellite Orbits*, National Aeronautics and Space Administration, Washington D.C. 2009. Available at: https://earthobservatory.nasa.gov/features/OrbitsCatalog (accessed: 02/02/2025).

Rieder, B., Sire, G., *Conflicts of interest and incentives to bias: A microeconomic critique of Google's tangled position on the web, New Media and Society*, 2013, 16(2), pp. 195–211.

Ross, A., Kenya's Safaricom urges new requirements for satellite providers like Starlink, *Reuters*, 23 August 2024. Available at: https://www.reuters.com/business/

media-telecom/kenyas-safaricom-urges-new-requirements-satellite-providers-like-starlink-2024-08-23/ (accessed: 30/10/2024).

Rosson Z., Tackett C., Felicia, The Most Violent Year: Internet Shutdowns in 2023, *Access Now*. Available at: https://www.accessnow.org/internet-shutdowns-2023/ (accessed: 06/11/2024).

Safaricom, *Safaricom Increases Internet Speeds For Home And Business Customers, Introduces The New 1000Mbps Platinum Package For Customers*, 23 September 2024. Available at: https://www.safaricom.co.ke/media-center-landing/press-releases/safaricom-increases-internet-speeds-for-home-and-business-customers-introduces-the-new-1000mbps-platinum-package-for-customers (accessed: 30/10/2024).

Sehloho, M., South Africa could amend law blocking Starlink entry, *Connecting Africa*, 8 October 2024. Available at: https://www.connectingafrica.com/regulation/south-africa-could-amend-law-blocking-starlink-entry (accessed: 11/11/2024).

Sen, R., Ahmad, S., Phokeer, A., Farooq, Z.A., Qazi, I.A., Choffnes, D., Gummadi, K.P., Inside the walled garden: Deconstructing Facebook's Free Basics program, *SIGCOMM Computer Communication Review*, 2017, 47(5), pp. 12–24, https://doi.org/10.1145/3155055.3155058

Shaengchart, Y., Kraiwanit, T., Starlink satellite project impact on the internet provider service in emerging economies, *Research in Globalization*, 2023, 6, pp. 1–7, https://doi.org/10.1016/j.resglo.2023.100132

Shanahan, M., Bahla, K., *The State of Mobile Internet Connectivity 2024*, Global System for Mobile Communications Association, London 2024, p. 5. Available at: https://www.gsma.com/r/wp-content/uploads/2024/10/The-State-of-Mobile-Internet-Connectivity-Report-2024.pdf (accessed: 21/10/2024).

Signé, L., Africa's Consumer Market Potential, *Brookings*, 12 December 2018. Available at: https://www.brookings.edu/articles/africas-consumer-market-potential/ (accessed: 07/11/2024).

Starlink, *Availability Map*. Available at: https://www.starlink.com/map (accessed: 27/10/2024).

Starlink, *Satellite Technology*, 2024. Available at: https://www.starlink.com/technology (accessed: 11/11/2024).

Starlink, *SpaceX Sends First Text Message Via Its Newly Launched Direct to Cell Satellites*, 10 January 2024. Available at: https://api.starlink.com/public-files/DIRECT_TO_CELL_FIRST_TEXT_UPDATE.pdf?_gl=1*1xtmfc*_ga*MTE1NDY0MDE4NC4xNzI2MDYyMzk0*_ga_S07SYD5D4F*MTczMDMwMTc4MC4xMi4wLjE3MzAzMDE3ODAuMC4wLjA. (accessed: 09/11/2024).

Starlink, *Specifications*. Available at: https://www.starlink.com/specifications?spec=5 (accessed: 11/11/2024).

United Nations Economic Commission for Europe, *UN/LOCODE code list by country and territory*, UNECE, 30 July 2024. Available at: https://unece.org/trade/cefact/unlocode-code-list-country-and-territory (accessed: 11/11/2024).

Wang, **Y., Ding, X., Zhang, G.**, A novel dynamic spectrum-sharing method for GEO and LEO satellite networks, *IEEE Access*, 2020, 8, pp. 147895–906. https://doi.org/10.1109/ACCESS.2020.3015487

Weston, S. (ed.), *Small Spacecraft Systems Virtual Institute: Small Spacecraft Technology State-of-the-Art Report*, NASA Ames Research Center, Moffett Field 2024, pp. 243–251. Available at: https://www.nasa.gov/wp-content/uploads/2024/03/soa-2023.pdf?emrc=8ad1a1 (accessed: 24/10/2024).

The White House, *The National Spectrum Strategy*, 13 November 2023, pp. 9–10. Available at: https://www.ntia.gov/sites/default/files/publications/national_spectrum_strategy_final.pdf (accessed: 11/11/2024).

World Bank Group, *From connectivity to services: Digital transformation in Africa*, 2023. Available at: https://projects.worldbank.org/en/results/2023/06/27/from-connectivity-to-services-digital-transformation-in-africa (accessed: 11/11/2024).

Yadav, A., Manthan, A., Somya, A., Sachin, V., *Internet From Space Anywhere and Anytime – Starlink*, 2nd International Conference on "Advancement in Electronics & Communication Engineering", 2022, pp. 480–487. Available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4160260 (accessed: 11/11/2024).

Yadav, A., Agarwal, M., Agarwal, S., Verma, S., Internet from space anywhere and anytime—*Starlink. Proceedings of the Advancement in Electronics & Communication Engineering*, 2022, July, pp. 1–8.

Yieke, L., Starlink's Aggressive Push in Africa Keeps Telcos on High Alert, *African Business*, 1 November 2024. Available at: https://african.business/2024/11/technology-information/starlinks-aggressive-push-in-africa-keeps-telcos-on-high-alert (accessed: 02/05/2025).

Zandt, F., Infographic: SpaceX triples number of rocket launches in two years, *Statista*, 14 October 2024. Available at: https://www.statista.com/chart/29410/number-of-worldwide-rocket-launches-by-companies-and-space-agencies/ (accessed: 06/11/2024).

SECTION IV

https://doi.org/10.18778/8331-719-9.12

Insights from the Internet – How to Govern Outer Space

Mallory Knodel[1]

Introduction

As the space domain grows more congested and complex, the need for robust governance frameworks becomes increasingly urgent. The challenges of managing orbital traffic, sharing critical space situational awareness (SSA) data, and fostering collaboration among a small but very diverse set of stakeholders—governments, industry, and civil society—mirror similar struggles faced by the Internet in its early days.[2] Many have pointed out the parallels between space and internet governance from legal and regulatory perspectives.[3]

Starting in the 1980s, internet governance evolved to manage the global, decentralized nature of a network that connects billions of devices, applications, and users. Multistakeholderism can be exemplified by organizations like the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Engineering Task Force (IETF), which have created a constellation of global governance ecosystems that promote interoperability through technical standards, foster collaboration at fora events, and ensure that no single entity dominates decision-making through policy development. Similarly, the space community must

1 New York University, United States.

2 Secure World Foundation, *Handbook for New Actors in Space*. Secure World Foundation, Broomfield, Colorado 2024. Available at: https://swfound.org/media/207931/handbook-for-new-space-actors_2024-revision.pdf (accessed: 25/02/2025).

3 J. Malcolm, The Space Law Analogy to Internet Governance, *SSRN Scholarly Paper*, Rochester, New York 2008. Available at: https://papers.ssrn.com/abstract=2798396 (accessed: 25/02/2025).

grapple with how to establish shared norms and practices that balance the interests of national governments, private operators, and other stakeholders.[4]

There is a growing number and diversity of actors in space, ranging from governments to private companies and end-users reliant on space-based data. There is an urgent need to address these challenges, for example, shared (or the lack of) SSA data nears a "tipping point" where collisions and congestion could become increasingly unmanageable without coordinated action. Rather than coming together, the SSA ecosystem is fragmenting as nations and companies develop independent systems that lack interoperability or shared standards.

The Internet governance model, while not perfect, offers valuable lessons for addressing these potential fragmentations. The Internet operates as a "network of networks," interconnected through shared protocols realistically only one: the Internet Protocol—and guided by governance structures that prioritize inclusivity and consensus-building but that are pluralistic and complex as a whole. By adopting similar principles and embracing complexity, the space community can work toward a sustainable governance model that seeks to ensure safety, transparency, and equity for all actors operating in orbit.

The following analysis explores how the principles of Internet governance can inform the development of space governance systems. It examines the successes and shortcomings of multistakeholder approaches in the Internet domain and considers their applicability to pressing issues in space, such as SSA data sharing, standardization, and the inclusion of diverse voices in decision-making. Ultimately, this author argues that the space community can leverage existing internet governance fora and processes to achieve consensus on select aspects of space governance that overlap with telecommunications, and at the same time it must take active steps to create a framework that ensures the long-term sustainability of the orbital environment by embracing the lessons of Internet governance.

Background

Internet operators connect billions of people and services through a set of shared protocols, the main one being TCP/IP, which enables seamless communication across networks through a narrow waistband of interoperability. Furthermore, it relies on decentralization and permissionless innovation enabled by two other crucial protocols: the Border Gateway Protocol (BGP) for lightweight global routing and the Domain Name System (DNS) for global identifiers. But the internet is far from simple in its construction, maintenance and growth: it is built upon consensus-driven governance to maintain its technical standards and operational stability.[5]

4 M. Knodel, U. Uhlig, *How the Internet Really Works*, No Starch Press, San Francisco 2020. Available at: https://nostarch.com/how-internet-really-works (accessed: 25/02/2025).

5 *Ibidem*.

The key parallels between the internet and space are: global commons with decentralized actors, requirements for interoperability, data sharing, and governance; and the need to solve common hard problems of accountability and resource management.

Space and the internet diverge on the robustness of cooperation and governing documents. On the one hand, from engineers to CEOs there are millions of people working together to keep the internet running, and only a few governments and companies actively operating in space. On the other hand, there are no major treaties that underpin the global internet, and many people have considered the five space treaties[6] as definitive of space governance. However, there are new developments happening at the ITU where aspects of internet and telecommunications are also discussed. For example the ITU Radio Regulations (RR) advanced as recently as 2019 for non-geostationary satellite systems and in 2023 for company's jurisdictional requirements, together enabling the "new applications of radiocommunication technology while ensuring the efficient use of radio-frequency spectrum, i.e. the operation of as many systems as possible, without interference."[7]

From Cyberspace to Outer Space

Space governance can draw directly from the Internet's successes, particularly its emphasis on shared protocols, multistakeholder collaboration, and adaptive standards. However, these principles must be tailored to space's unique challenges, such as its physical constraints and the predictive nature of orbital management.

Protocols and standards

What does it mean to be on the internet? Surprisingly the only thing connecting us is the internet Protocol. Most other elements of any Internet service are left up to specific implementations, which are built upon norms and other protocols, but which can and do evolve over time.

It's helpful to visualize the Internet through the 'hourglass model.' At the bottom, you have hardware—things like satellites, undersea cables, and network cards. At the top, you have user-facing applications and platforms. The narrow middle, where TCP/IP exists, is the critical protocol that connects it all. This layer is key because it's both simple and universal. It allows any network—no matter how bespoke or localized—to connect to the broader Internet seamlessly.

---

6 R.P. Rajagopalan, *The Outer Space Treaty: Overcoming Space Security Governance Challenges*, Council on Foreign Relations, Washington D.C. 2021.

7 ITU, *Non-Geostationary Satellite Systems*, New York 2021. Available at: https://www.itu.int:443/en/mediacentre/backgrounders/Pages/Non-geostationary-satellite-systems.aspx (accessed: 25/02/2025).

Governance builds out from this narrow protocol layer. Governance is about supporting technology innovation and use, addressing thorny issues that everyone has like spam or infrastructure replacement, and allowing diverse stakeholders—governments, companies, and even communities—to contribute to solving those problems. SSA standardization and other emerging technologies for satellite Internet constellations (SICs) are desperately needed and yet unattainable for largely non-technical reasons.[8]

Multistakeholder governance

Compliementary to technical specifications is defining the shared values, coming to consensus on norms and recognizing that the real asset for any global system is the robust network of people and their relationships to one another.

Multistakeholder governance ensures that those actively involved in building and operating systems also have a say in decision-making. For example, the IETF and ICANN work through open and inclusive processes. Anyone can join the IETF mailing lists or participate in meetings, which are fully open and free. ICANN, which oversees domain names and numbers, operates through contracts rather than ownership, ensuring accountability and interoperability.

This model recognizes that governments alone cannot address all challenges. In fact, some governments in the Global South have less capacity to engage in Internet governance than some nonprofit organizations or companies. Embracing the diversity of actors—from civil society to businesses—is key to solving complex problems.

Safety and accountability

Dealing with bad actors is a persistent challenge. On the Internet, we balance the principle of "connectivity at all costs" with efforts to curb spam and state-led censorship. For instance, multistakeholder organizations like the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) address spam, while diplomatic efforts counter state interference. The Certificate Authorities (CA) collectively ensure trust and accountability in the web through shared principles.

At the same time, space governance faces its own unique challenges, such as the predictive nature of space traffic management and the need for real-time, accurate data.

Standards and best practices are essential, but the key insight is to identify what should be standardized and how as a matter of priority. While stakeholders

8 J. Leiken, Satellite internet and laser links: Are universal FSO standards needed?, *New York University Journal of Legislation and Public Policy*, 2024, 26, p. 1165.

might operate differently, collaboration—across governments, companies, and other actors—creates stronger systems. For instance, in the Internet world, even small community-driven networks can connect globally using universal protocols. Space governance could adopt similar principles to manage the growing number of actors and ensure shared accountability. Prioritizing an issue like safety in space can help to focus stakeholders and strengthen the consensus-building process in early stages.

Transparency and equity

There are major milestones in Internet governance that can offer valuable insights for space sustainability. The transition of ICANN from U.S. government control to a global multistakeholder process shows how shared governance can work, but that if possible this sort of transition moment can be avoided entirely.

The lesson for space governance is the importance of fostering cooperation. While enforcement is difficult, building consensus and adopting shared standards helps mitigate the risks of bad behavior. Ultimately, inclusivity and collaboration within a truly multistakeholder governance process make systems more resilient.

Discussion

One of the critical lessons from internet governance is the power of norms and standards. In the absence of formal treaties, the Internet community has developed consensus-driven processes to create guidelines and technical standards that ensure interoperability, security, and access. These norms have helped to balance competing interests while preserving the Internet as a global public good. Similarly, space governance needs to embrace norm-setting as a way to manage the responsible and equitable use of space, particularly as private actors increasingly dominate the field.

Another parallel lies in the challenges of access and security. Just as we've grappled with issues of digital inclusion and cybersecurity, space governance must address questions about who gets to use space, how resources are allocated, and how we prevent monopolistic control. Left unchecked, the commercialization of space could lead to outcomes that serve the few at the expense of the many, much like the consolidation of power we've seen among a handful of internet platforms.

Perhaps one area with sharp departure from internet governance is the potential for kinetic and other real-world conflict, intentional or accidental, in space. Much of the scholarship related to space law is concerned with the "final frontier" for military action. "[G]rey zone conflict in outer space is closely linked to a persistent

failure to adequately govern peaceful space activities."[9] The role of space Internet in connected warfare and algorithmically driven weapons, an area where Internet governance is not sufficiently covered by expertise or binding agreements.[10]

The governance models that have enabled the internet to thrive—though not without flaws—offer a valuable blueprint for space governance. However, it is not enough to simply replicate these models; they must be adapted to the unique context of space. This includes recognizing the different technological, legal, and political landscapes, as well as the fact that space, unlike the internet, is a physical frontier with finite resources.[11]

Practically, what should be of priority for states and companies investing in space:

1. Leverage existing paradigms of international collaboration where there exists technology crossover, such as internet and telecommunications as well as the International Space Station.
2. Choose the minimum viable protocols for ground truth and governance (like GPS, BGP routing, and CAs), treat them as public interest goods and collaborate to ensure their collective governance, such as SSA and SIC standards.

These expert communities need an iterative, consensus-driven approach to space governance, one that builds on the principles of openness, inclusivity, and accountability. By involving a broad range of stakeholders and fostering a culture of collaboration, we can ensure that space remains a resource for all humanity, not just those with the most power or capital.

Recommendations

A succinct list of recommendations from the analysis and discussion that are based on decades of internet governance include:

- Establish shared values such as rule of law, economic systems, human rights.
- Rather than new treaties, focus on shared work and building consensus on technical standards that are sensitive to equitable governance among stakeholders.
- Identify existing standards overlap with telecommunications, such as GPS, DTN, satellite Internet delivery and work on those standards within fora that are already multistakeholder, such as the IETF, or have the potential to be, such as the ITU with Observer Memberships or the Consultative Committee for Space Data Systems (CCSDS).

9 J. West, J. Miller, *Grey Zones in Space Governance. Clearing the Fog*, Centre for International Governance Innovation, Washington D.C. 2023.

10 M. Knodel, *Comments to the United Nations on the Global Digital Compact*, Center for Democracy and Technology, Washington D.C. 2024. Available at: https://cdt.org/insights/comments-to-the-united-nations-on-the-global-digital-compact/ (accessed: 25/02/2025).

11 L. DeNardis, *Interplanetary Internet Governance*, CIGI Paper No. 277, Center for International Governance Innovation, Washington D.C. 2023. Available at: https://www.cigionline.org/publications/interplanetary-internet-governance/ (accessed: 25/02/2025).

- Ensure new standard protocols are safety minded: The architecture that is maximally interoperable needs to be permissionless, such as SSA and SICs.
- Identify and protect public goods, like GPS, through proper governance.
- Make the case for an initial focus on safety, including issues affected by war and disaster.
- Equitable governance means a willingness to hold companies accountable.
- Address what isn't working in the current structure head on: First come first served is colonialist. There aren't enough incentives among powerful states to cooperate. Without standards there is no ground truth.[12]

In conclusion, the nascent field of space governance can—and should—draw heavily from the lessons learned in internet governance. There are strong parallels between the challenges in managing the global internet and those now surfacing in the governance of outer space.[13] The stakes are high, and the opportunity to shape the governance of the space frontier should not be taken in earnest. Together we can leverage the existing governance framework of the internet as well as create a new space governance framework, both of which should reflect our shared values and aspirations for the future of humanity.

Bibliography

Davis, N., End 'colonial' approach to space exploration, scientists urge, *The Guardian*, 4 March 2023. Available at: https://www.theguardian.com/science/2023/mar/04/end-colonial-approach-to-space-exploration-scientists-urge (accessed: 25/02/2025).

DeNardis, L., *Interplanetary internet governance*, CIGI Paper No. 277, Center for International Governance Innovation, Washington D.C 2023. Available at: https://www.cigionline.org/publications/interplanetary-internet-governance/ (accessed: 25/02/2025).

International Telecommunication Union (ITU), *Non-geostationary satellite systems*, ITU, 2021. Available at: https://www.itu.int:443/en/mediacentre/backgrounders/Pages/Non-geostationary-satellite-systems.aspx (accessed: 25/02/2025).

Kennedy, B., **Tyson, A.**, *Americans' views of space: U.S. role, NASA priorities and impact of private companies*, Pew Research Center 2023. Available at: https://www.pewresearch.org/science/2023/07/20/americans-views-of-space-u-s-role-nasa-priorities-and-impact-of-private-companies/ (accessed: 25/02/2025).

12 N. Davis, End 'colonial' approach to space exploration, scientists urge, *The Guardian*, 4 March 2023. Available at: https://www.theguardian.com/science/2023/mar/04/end-colonial-approach-to-space-exploration-scientists-urge (accessed: 25/02/2025).

13 Secure World Foundation, *5th Space Sustainability Summit in New York City*. Secure World Foundation, New York 2023. Available at: https://swfound.org/events/2023/5th-space-sustainability-summit-in-new-york-city (accessed: 25/02/2025).

Knodel, M., Comments to the United Nations on the global digital compact. *Center for Democracy and Technology*, Washington D.C. 2024. Available at: https://cdt.org/insights/comments-to-the-united-nations-on-the-global-digital-compact/ (accessed: 25/02/2025).

Knodel, M., **Uhlig, U.**, *How the Internet Really Works*, No Starch Press, San Francisco 2020. Available at: https://nostarch.com/how-internet-really-works (accessed: 25/02/2025).

Leiken, J., Satellite internet and laser links: Are universal FSO standards needed?, *New York University Journal of Legislation and Public Policy*, 2024, 26, p. 1165.

Malcolm, J., The space law analogy to internet governance, *SSRN Scholarly Paper*, Rochester, New York 2008. Available at: https://papers.ssrn.com/abstract=2798396 (accessed: 25/02/2025).

Rajagopalan, R.P., *The Outer Space Treaty: Overcoming space security governance challenges*, Council on Foreign Relations, Washington D.C. 2021.

Secure World Foundation, *5th space sustainability summit in New York City*, Secure World Foundation 2023. Available at: https://swfound.org/events/2023/5th-space-sustainability-summit-in-new-york-city (accessed: 25/02/2025).

Secure World Foundation, *Handbook for new actors in space*. Secure World Foundation 2024. Available at: https://swfound.org/media/207931/handbook-for-new-space-actors_2024-revision.pdf (accessed: 25/02/2025).

West, J., **Miller, J.**, *Grey zones in space governance: Clearing the fog*. Centre for International Governance Innovation, Washington D.C. 2023.

https://doi.org/10.18778/8331-719-9.13

Conclusions

Joanna Kulesza, Berna Akcali Gur

The expansion of Low Earth Orbit satellite technology presents critical challenges that demand immediate attention. As satellite systems reshape global connectivity, security, and economic structures, existing legal frameworks must evolve to ensure effective governance. Without an interdisciplinary approach, current policies risk being inadequate in addressing emerging cybersecurity threats, digital sovereignty concerns, and geopolitical tensions. The priority must shift toward ensuring that governance mechanisms balance end users' interests against more prevalent corporate or state interests.

The reliance on space treaties that establish broad principles and fragmented regulatory frameworks creates substantial challenges in managing the rapid expansion of satellite numbers and space-based activity. As a result, significant gaps exist in addressing the complex and evolving needs of satellite regulation and governance with commercial actors taking the lead in satellite deployment, issues such as market monopolization, orbital congestion, and equitable access require urgent international coordination. Economic policies and governance structures must adapt to these realities, ensuring that innovation does not outpace regulation. Without clear rules, private enterprises could dominate access to space resources in a way that prioritises their commercial targets, limiting present and future opportunities for global sustainable and equitable development and creating new forms of digital dependency for less technologically advanced nations. The current regulatory landscape remains focused on state actors, failing to fully incorporate the commercial space industry's increasing influence and role in shaping contemporary space governance. The privatization of satellite networks calls for policies that prevent exploitation while encouraging innovation balancing economic incentives with public interest safeguards.

The rapid growth of satellite networks also amplifies cybersecurity risks. Without comprehensive legal mechanisms, vulnerabilities in satellite infrastructure risk data breaches, cyber warfare, and system failures with global implications. The increasing reliance on privately owned satellite networks for governmental,

commercial, and civilian purposes makes it imperative to establish regulatory oversight that is both adaptive and enforceable. Cyber threats originating from state and non-state actors require coordinated policy responses that integrate cybersecurity standards with international legal frameworks. Additionally, questions of digital sovereignty must be addressed to prevent overreliance on a handful of powerful entities that control access to essential services, raising concerns over jurisdiction, data ownership, and the ability of individual states to ensure their own security and economic stability. The fragmentation of global cybersecurity regulations further exacerbates vulnerabilities, highlighting the need for collaborative frameworks that facilitate information-sharing and coordinated responses to cyber threats.

The use of satellites by states with varying governance models highlights the risks of technological misuse. Some governments are more likely to leverage satellite systems as part of their surveillance and information control infrastructure. The dual-use nature of satellite technology means that the same infrastructure designed to improve connectivity and facilitate economic growth can also be weaponized for strategic military advantages or political suppression. Global legal structures must balance national security interests with human rights protections, ensuring satellite technology is used responsibly. Without proper oversight, these tools could exacerbate geopolitical tensions rather than bridge digital divides. The lack of universally accepted norms governing the responsible use of satellite data further complicates efforts to mitigate these risks, emphasizing the need for international cooperation in the development of ethical and legal guidelines. The intersection of space law, cyber law, and human rights law underscores the necessity of interdisciplinary approaches that incorporate principles of transparency, accountability, and fairness in satellite governance.

Current regulatory efforts often lack the interdisciplinary collaboration needed to address real-world implications. Satellite governance should integrate input from law, technology, policy experts, and human rights to create adaptable and forward-thinking frameworks. The scope of new space law instruments must be expanded in consideration of economic justice, cybersecurity resilience and environmental sustainability. Spacefaring nations should adopt these instruments. The increasing congestion of orbital pathways presents long-term risks, including the growing threat of space debris that could endanger current and future satellite operations. International institutions must facilitate cross-sector discussions that prioritize practical solutions over bureaucratic inefficiencies. This approach ensures that governance structures are not only legally sound but also technically feasible and aligned with user needs. Technical experts, economists, and human rights advocates should collaborate with legal scholars to craft policies that reflect the complexities of modern satellite use, ensuring that regulations keep pace with technological advancements rather than reacting to crises after they arise. The integration of technical expertise in legal discourse is critical to crafting solutions

that are both feasible and enforceable, preventing regulatory stagnation in an industry that continues to evolve at a rapid pace.

As reliance on satellite technology grows, end-user interests must be central to governance discussions. This approach includes ensuring equitable access to satellite communications, protecting privacy, and preventing economic exploitation. The development of legal frameworks must account for those who depend on satellite services the most, including remote and underserved communities. The digital divide remains a pressing issue, and while satellite broadband has the potential to expand internet access, market-driven pricing models often place these services out of reach for marginalized populations. Without regulatory intervention, commercial satellite operators may continue to prioritize profitability over equitable access. Regulatory bodies should focus on creating policies that are transparent, inclusive, and responsive to technological advancements. The role of multistakeholder governance in shaping policies that reflect both technical realities and societal needs cannot be overstated. The interests of corporations, governments, and civil society organizations must be balanced to create frameworks that are both enforceable and adaptable to the dynamic nature of satellite technology. Public-private partnerships, regulatory innovation, and participatory decision-making processes must be explored as mechanisms to create governance models that effectively address the interests of all stakeholders.

The urgency of satellite governance requires a shift toward interdisciplinary, user-focused solutions. Existing treaties and regulations must evolve to meet the needs of modern satellite technology, moving beyond the foundational agreements that were designed for a space environment dominated by state actors. Collaboration between international organizations, governments, and private actors is essential for effective governance. Private sector involvement in space infrastructure has introduced efficiency and innovation but has also created new regulatory challenges that require oversight to ensure accountability. Technical and legal safeguards must be established to protect satellite networks from cyber threats, data breaches, and operational failures. Policies must be structured to prevent monopolization and support fair global connectivity, ensuring that the benefits of satellite expansion are not disproportionately concentrated among wealthier nations and corporate entities. Space governance should prioritize human rights and transparency, mitigating risks associated with state and corporate control. Issues such as the militarization of space, the commodification of data, and the environmental impact of satellite launches must be examined within the context of international law and policy frameworks. The importance of environmental considerations in satellite governance is growing, as space debris and unsustainable launch practices pose long-term threats to global space infrastructure. The establishment of environmental protocols specific to LEO satellites is critical in ensuring the long-term sustainability of satellite operations.

The expansion of satellite networks offers both opportunities and risks. Without an interdisciplinary, forward-thinking approach, governance structures will

fail to keep pace with technological advancements. The international community must act now to develop legal and policy frameworks that prioritize end-user needs, ensuring that satellites contribute to global connectivity and security rather than deepening existing inequalities. Without proactive legal and policy measures, the opportunity to create an inclusive and sustainable satellite ecosystem may be lost, reinforcing existing power imbalances and restricting access to critical digital resources. The need for international cooperation in space governance has never been more urgent. Stakeholders across legal, technical, and policy fields must work together to shape a future where satellite technology serves as a tool for equitable global development rather than a mechanism for control and exclusion. Time is running out to establish practical, inclusive solutions before regulatory gaps become insurmountable, and failing to act now could result in consequences that extend far beyond space policy into the broader fabric of global governance. The future of global connectivity, economic equity, and digital sovereignty will be determined by the choices made today in crafting adaptive and enforceable satellite governance frameworks.

A first comprehensive volume dedicated to the global governance of satellite connectivity, this work is both original and innovative, addressing critical challenges for policymakers and scholars alike.

— Professor Roxana Radu, Associate Professor, Blavatnik School of Government, University of Oxford

This volume fills a critical gap in scholarship by bringing legal, policy, and technical perspectives into a cohesive debate on the global governance of LEO satellites.

— Dr Jamal Shahin, Chair of the Global Internet Governance Academic Network (GigaNet), Programme Director of the Advanced Master European Integration, Brussels School of Governance, and Professorial Fellow, UNU-CRIS

This landmark volume offers a rigorous interdisciplinary examination of the governance challenges posed by the rapid expansion of Low Earth Orbit satellite constellations. Featuring original research from leading and emerging experts, it bridges international law, Internet governance, and international relations to chart pathways toward equitable and sustainable space governance.

Generously supported by the Internet Society Foundation, this book is essential reading for academics, policymakers, and practitioners shaping the future of global digital infrastructure and space law.

WYDAWNICTWO UNIWERSYTETU ŁÓDZKIEGO

wydawnictwo.uni.lodz.pl
ksiegarnia@uni.lodz.pl
(42) 665 58 63

The book is also available as an e-book

ISBN 978-83-8331-718-2