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.

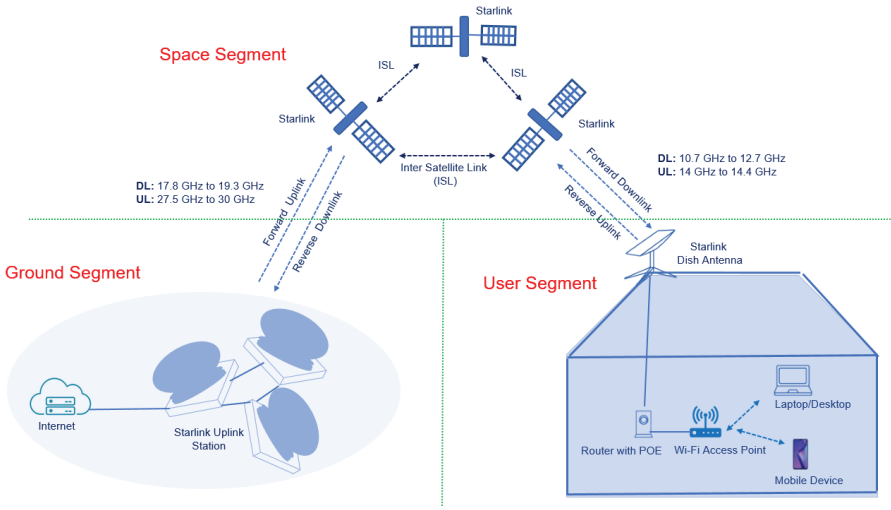

Fig. 1. A diagram of the key features of a satellite broadband system
Source: SpaceX – Starlink System Architecture for Internet, *Techplayon*, 12 January, 2024. Available at https://www.techplayon.com/starlink-system-architecture/ (accessed: 31/12/2024).

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.

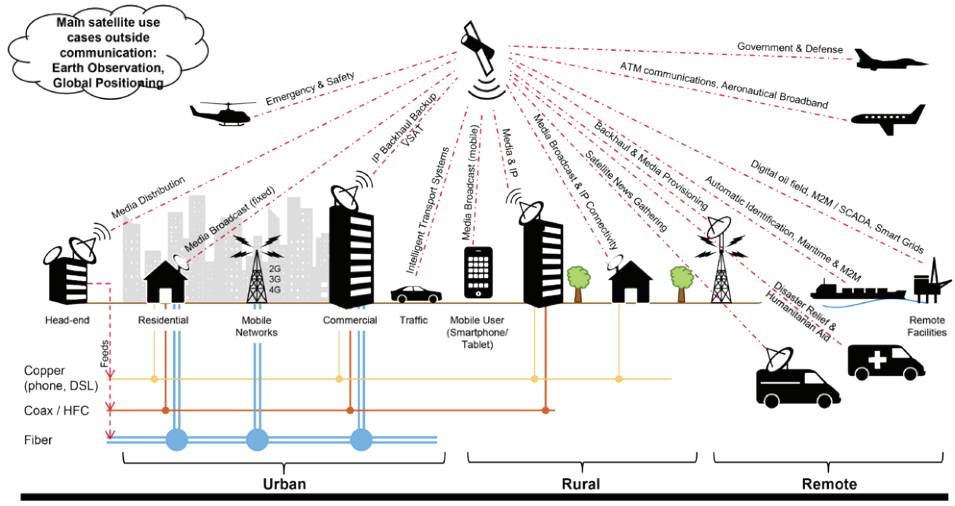

Fig. 2. Satellites' role in the global internet infrastructure
Source: S. Raman, R. Weigel, T. Lee, The Internet of Space (IoS): A Future Backbone for the Internet of Things?, *IEEE Internet of Things*, 8 March 2016. Available at: https://iot.ieee.org/articles-publications/newsletter/march-2016/the-internet-of-space-ios-a-future-backbone-for-the-internet-of-things.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 AC-TORS TO ESTABLISH A COMPREHENSIVE, RULES-BASED ORDER FOR LEO AC-CESS, PROMOTING GLOBAL CONNEC-TIVITY ALIGNED WITH SDGs	EFFECTIVE IMPACT ONTO FURTHER DE-VELOPMENT OF LEO RELEVANT POLICIES	RESOURCE-INTEN-SIVE: HUMAN RE-SOURCES, CAPACITY BUILDING, ACTIVE ENGAGEMENT	RECOMMENDED
OPTION 6	ENGAGED	"UNIVERSAL LEOs"	ACTIVELY ENGAGE IN EXISTING INTER-NATIONAL AND RE-GIONAL FORUMS TO ENSURE POLICIES FACILITATE GLOBAL CONNECTIVITY AND SUSTAINABLE DE-VELOPMENT 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).