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.