

# *Map of Space Threats and Consequences*

**Applied Research Project 32**

## **Final Report**

**Aryan Bajpai,  
Linnéa Batey Skoglund,  
Mehmet Fatih İzgi,  
Paula Monteiro Barioni**

**May 16th, 2025**

**Partner Institution: United Nations Institute for Disarmament Research  
(UNIDIR)**

**Faculty Lead: Dr. Jérôme Duberry**

**Word count: 11,000**

**Disclaimer:** This report was prepared by Geneva Graduate Institute (IHEID) students as part of an academic research project during their studies. It does not imply the expression of any opinion on the part of the United Nations, the United Nations Institute for Disarmament Research (UNIDIR) or IHEID concerning the legal status of any country, territory, or area, or of their authorities. The views expressed in this publication are those of the authors and do not necessarily reflect the views of the United Nations, UNIDIR, its staff, its sponsors, or IHEID.

## Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Introduction</b>	<b>2</b>
<b>Methodology</b>	<b>3</b>
<b>Context</b>	<b>4</b>
<b>Literature Review</b>	<b>7</b>
<b>Space Threats</b>	<b>8</b>
(i) Political Threats	9
a) Geopolitical Context	9
b) States' Interpretation of "Threat" Concept in the Context of Space Law	12
(ii) Ground-to-Space Threats	16
a) Direct-ascent missiles	16
b) Ground-based directed energy weapons	18
(iii) Space-to-Ground Threats	18
a) Nuclear detonation from space	19
b) Space-based directed energy weapons	20
c) Kinetic bombardment	20
(iv) Space-to-Space Threats	20
a) Co-Orbital ASATs	21
b) Dual-Purpose Objects	22
c) The Sustainable use of Space	25
(v) Ground-to-Ground Threats	28
a) Sabotage	29
b) Attacks on ground stations and terrorism	30
a) Espionage	30
(vi) Cyber Threats	32
<b>Consequences for Space and Earth</b>	<b>36</b>
Consequences for Space	36
Short Term Consequences	36
Long Term Consequences	37
Consequences for Earth	38
Short Term Consequences	38
Long Term Consequences	40
<b>Conclusion</b>	<b>42</b>
<b>Bibliography</b>	<b>44</b>
<b>Annex</b>	<b>55</b>

# Introduction

Space is an integral and indispensable part of all our lives on Earth, and should not be seen as something relevant only in movies or science fiction, but rather as a vital tool that enables the use of services that are used in all parts of life. From using location services as one tries to find their way back home, checking the weather forecasts when getting dressed in the morning, messaging a friend, or paying for a ticket on public transport, these are all everyday activities that rely on access to Space and Space-based systems.<sup>1</sup>

Not all States are equally space-faring or have their technologies in space, but all humanity relies on space systems. The increased reliance on Space systems has led us to the emergence of space security and concern about the role of possible space threats.<sup>2</sup> Regarding space security, we are concerned about the "relationship among space objects and activities and the maintenance of international peace and security, as well as disarmament, including the prevention of an arms race in outer space."<sup>3</sup> This research has aimed to identify what kind of threats not only States but also stakeholders should be concerned about, and what the possible consequences of these are, not only in Space but also for us on Earth. The following research questions have guided our research:

- What threats to space systems should States and other stakeholders be concerned about?
- What are the consequences of the denial, disruption, degradation, damage or destruction of space systems for (i) outer Space; and (ii) Earth?

Space is becoming increasingly militarized. This is not necessarily a new concept, the militarization of space refers to the use of Outer Space for military purposes, such as early warning systems, data gathering, communication, and navigation. What is emerging is the increasing discussion on the *weaponization* of Space, which involves placing destructive

---

<sup>1</sup> Rian Davis, Brianna Bace, and Unal Tatar, "Space as a Critical Infrastructure: An in-Depth Analysis of U.S. and EU Approaches," *Acta Astronautica* 225 (December 2024): pp.269-270, <https://doi.org/10.1016/j.actaastro.2024.08.053>.

<sup>2</sup> Cassandra Steer, "Global Commons, Cosmic Commons: Implications of Military and Security Uses of Outer Space," *Georgetown Journal of International Affairs* 18, no. 1 (2017): p.11, <http://www.jstor.org/stable/26396047>.

<sup>3</sup> Space Security - Terminology - Outer Space Security Lexicon," <https://spacesecuritylexicon.org/terminology/space-security>.

weapons into Outer Space itself.<sup>4</sup> This shift is particularly relevant as we observe space activities transitioning from traditional militarization toward potential weaponization. This represents a shift from "danger" toward "threat" in the space security context.<sup>5</sup>

This research report will begin by outlining our general methodology and providing a brief on the general, historical, and legal context of space. There will be a subsequent overview of literature and its limitations before delving into evaluated threats. These are Political, Ground-to-Space, Space-to-Ground, Space-to-Space, and Ground-to-Ground. Lastly, we will finish with the role of Cyber and Electronic threats. Then, we will examine the consequences this has in the short-term and long-term, both for Space and on Earth.

---

## Methodology

We adopted a multidimensional methodological approach, with a combination of desk research, interviews, and participation in specialized conferences on the subject. We chose this methodology to promote a detailed analysis that accounts for the complexities involved in research on space-related literature. We conducted desktop, documentary research on the topics contained in the research questions as a first step of the study, through exploratory research -mainly secondary research- on the existing literature in order to build a solid theoretical basis. At the same time, we searched for relevant United Nations institutional processes, documents, reports and UNIDIR publications. Once we established a theoretical understanding of the topic and understand what material States produce on space threats, we delved deeper into the sources that address and assess threats to space security.

The second stage consisted of conducting direct semi-structured interviews with key interviewees seeking data on the perceptions and experiences of participants, ensuring greater diversity and, above all, representation of different experts on space threats. The approach we used was the snowball sampling method, in which we found and interviewed a small pool of specialists who

---

<sup>4</sup> Saadia Zahoor, "Maintaining International Peace and Security by Regulating Military Use of Outer Space." *Policy Perspectives* 14, no. 2 (2017): p.122. <https://doi.org/10.13169/polipers.14.2.0113>.

<sup>5</sup> Space Security - Terminology - Outer Space Security Lexicon."

then indicated the next interviewees, ensuring we have diverse opinions on the topic, minimizing, as much as possible, possible biases and inclinations that could compromise the impartiality of the project. Our research did not require quantitative methods of inquiry. First, we asked them the initial questions found in the Annex, such as “In your opinion, what are the most pressing threats concerning space today?” and “Are current legal frameworks enough to address the existing threats?” We adapted our next questions to their responses. We also consulted them about how they see the advancement of international cooperation to mitigate the risks involving the use and exploration of space. With prior consent, the interviews were recorded to enable better analysis and later study. All information provided by the interviewees is confidential in our report unless express consent was given, which can be revoked at any time.

---

## Context

Human activity in space began as part of the Cold War as both sides vied to obtain a military advantage through the intelligence, reconnaissance and surveillance potential of space.<sup>6</sup> Within this period, the international legal framework governing space was established, spearheaded by the superpowers who wished to safeguard the military advantages they received.<sup>7</sup>

The framework for space activities is first articulated in the 1963 Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space (the Declaration), which the UN General Assembly adopted in Resolution 1963.<sup>8</sup> The Declaration is a non-binding instrument of soft law that may shape future treaties and has been referenced as customary international law. There were several important principles established in this document—peaceful use of outer space, non-appropriation, and international responsibility, for example—which were later codified into binding treaties. Moreover, the 1967 Outer Space Treaty (OST) can be considered the foundation of international space law. It notably prohibits national appropriation of outer space (including celestial bodies) and mandates that the

---

<sup>6</sup> Steer, p.9.

<sup>7</sup> Ibid, p.10.

<sup>8</sup> United Nations General Assembly. *Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space*. Resolution 1962 (XVIII), adopted December 13, 1963. [https://www.unoosa.org/pdf/gares/ARES\\_18\\_1962E.pdf](https://www.unoosa.org/pdf/gares/ARES_18_1962E.pdf).

exploration and use of outer space must be for the benefit of all mankind, and it imposes additional prohibitions against military activities in outer space by prohibiting weapons of mass destruction from being placed into orbit or establishing military bases, installations, or fortifications on celestial bodies.<sup>9</sup> In addition, pursuant to Article VI of the OST, States are required to bear international responsibility for national activities in outer space, whether performed by governmental or non-governmental entities, and must authorize and continually supervise such activities.

In order to further the development of the OST framework, later treaties addressed areas of law that were more particular in focus. The Rescue Agreement 1968<sup>10</sup>, elaborates upon Article V of the OST, obligating both the State that has jurisdiction over the recovery of distressed astronauts and the State that has responsibility for the safe return of the astronauts. The Convention on International Liability for Damage Caused by Space Objects (1972)<sup>11</sup>—commonly referred to as the Liable Convention—creates a two-tier regime of liability: liability for harm caused on the surface of the Earth or harm caused to an aircraft in flight is strict liability, while liability for damage caused in space is fault-based.

The Convention on Registration of Objects Launched into Outer Space (1976)<sup>12</sup> emphasizes transparency and accountability by obliging States to furnish information about their space objects to the United Nations—information that can be useful for managing space traffic and which will, at least in principle, inform oversight of national activities in space. While it remains non-binding on States, the Declaration of Legal Principles<sup>13</sup> adds greater depth to the notion of State accountability through reiterating the notion that activities must be conducted with due regard for the other States' interests.

---

<sup>9</sup> Gbenga Oduntan, *Sovereignty and Jurisdiction in the Airspace and Outer Space: Legal Criteria for Spatial Delimitation*, Routledge Research in International Law, London: Routledge, (2019).

<sup>10</sup> United Nations. *Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space*. Adopted December 19, 1967. Entered into force December 3, 1968. United Nations Treaty Series 672:119. [https://www.unoosa.org/pdf/gares/ARES\\_22\\_2345E.pdf](https://www.unoosa.org/pdf/gares/ARES_22_2345E.pdf).

<sup>11</sup> UN Office for Outer Space Affairs, “*Liability Convention (1972)*,” Accessed November 19, 2024, [https://www.unoosa.org/oosa/en/ourwork/spac and law/treaties/introliability-convention.html](https://www.unoosa.org/oosa/en/ourwork/spac%20and%20law/treaties/introliability-convention.html).

<sup>12</sup> UN Office for Outer Space Affairs, “*Registration Convention (1976)*,” Accessed November 20, 2024, <https://www.unoosa.org/oosa/sk/ourwork/spacelaw/treaties/introregistration-convention.html>.

<sup>13</sup> United Nations, “*Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space (1963)*,”

Other instruments must be also recognized, like the Moon Agreement (1979)<sup>14</sup>, which extends principles of the OST to the Moon and other celestial bodies, but has not achieved widespread acceptance and ratification in part due to its controversial notion that the resources of the Moon are the “common heritage of mankind”— a concept that few international actors accept. More broadly, the idea that outer space is a “global commons” is contested. This “global commons” framework has hence established space as a central piece of critical infrastructure<sup>15</sup> which incentivized the developing nations at the time, most significantly China and India, to also engage in space activities as a means of national development.<sup>16</sup>

A major shift came about with the first Gulf War in 1993, where the US military demonstrated the striking potential of space capabilities when it dominated through its “massive reliance on civilian satellite systems to accomplish military goals”<sup>17</sup>, exacerbated by the post-9/11 securitization of international politics, whereafter security implications of space became more emphasized than those of civilian or commercial interests.<sup>18</sup> This resulted in capacity building efforts of the militaries of major space powers, which most significantly materialized by the ASAT tests of China in 2007, US in 2008, India in 2019 and Russia in 2021.<sup>19</sup> Hence, the threat of conventional space weapons remains a significant possibility and a threat.<sup>20</sup>

---

<sup>14</sup> United Nations. *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*. Adopted December 5, 1979. Entered into force July 11, 1984. United Nations Treaty Series, vol. 1363, p. 3.

<https://treaties.un.org/doc/Publication/UNTS/Volume%201363/volume-1363-I-23002-English.pdf>.

<sup>15</sup> Jordan Plotnek and Jill Slay, “New Dawn for Space Security.” *International Conference on Cyber Warfare and Security* 17, no. 1 (March 2, 2022), p.258, <https://doi.org/10.34190/iccws.17.1.17>.

<sup>16</sup> Michael Sheehan. “Viewpoint: Space Security and Developing Nations.” *Space Policy* 37 (August 2016): p. 20, <https://doi.org/10.1016/j.spacepol.2016.10.005>.

<sup>17</sup> Michael Sheehan, “Viewpoint: Space Security and Developing Nations,” *Space Policy* 37 (August 2016): p.23, <https://doi.org/10.1016/j.spacepol.2016.10.005>.

<sup>18</sup> Wolfgang Rathgeber and Nina-Louisa Remuss. “Space Security. A Formative Role and Principled Identity for Europe,” European Space Policy Institute, January 16, 2009.

<https://www.espi.or.at/reports/space-security-a-formative-role-and-principled-identity-for-europe/>. p.4.

<sup>19</sup> Steer, p.11; Rajagopalan, p.60; Anelí Bongers and José L. Torres, “Star Wars: Anti-Satellite Weapons and Orbital Debris,” *Defence and Peace Economics* 35, no. 7 (2023): p.830. <https://doi.org/10.1080/10242694.2023.2208020>.; Dimitrios Strokos, “Still Lost in Space? Understanding China and India’s Anti-Satellite Tests through an Eclectic Approach,” *Astropolitics* 21 vol.2–3 (2023): p.179. <https://doi.org/10.1080/14777622.2023.2277253>.

<sup>20</sup> Dimitry V. Stefanovich, “Russia’s Vision for a Great Power Rivalry in Space.” *Journal of Space Safety Engineering* 10, no. 4 (December 2023): 538–43. <https://doi.org/10.1016/j.jsse.2023.10.007>, p.540

## Literature Review

Space is used for a large array of purposes. Initially, space activities had been limited to States, but private companies have played an increasingly larger role within the space sector.<sup>21</sup> The space services provided to the military have found a broader, more civilian and commercial appeal.<sup>22</sup> These appeals drew from capabilities like remote-sensing—which found wide use in agriculture and logistics by its ability to identify crops, insect swarms, meteorological events, etc.—and location and telecommunication services, which found great reception from both daily and business life, transforming modern societies and economies.<sup>23</sup> Today, most of the critical infrastructure is dependent on space services throughout the world.<sup>24</sup>

Space occupies an important place in international politics. It gave rise to a space regime based on an international legal framework centered around keeping space usable and accessible to all.<sup>25</sup> This has to do with the fact that confrontation regarding space has a unique character with wildly different implications to that of terrestrial confrontations<sup>26</sup> since destructive activity in space threatens all of humanity, including the perpetrator, because of the posterior risk posed by the creation of space debris.<sup>27</sup> Thus, discussions around space productively remained around minimizing the risk of confrontations by ensuring equitable access, the latest iteration of which is space sustainability.<sup>28</sup>

Yet, space is not wholly a peaceful domain. Inception of human space activity lies at the militarization of space, its use for military purposes, such as for intelligence gathering and surveillance, communication, early warning systems, and navigation.<sup>29</sup> This phenomenon is different to the weaponization of space, “the proliferation, testing, deployment and use of

---

<sup>21</sup> European Space Policy Institute, “The Rise of Private Actors in the Space Sector: Executive Summary,” (2017).

<sup>22</sup> Plotnek and Slay, p.253.

<sup>23</sup> Sheehan, 20

<sup>24</sup> Vessels et al, p.11.

<sup>25</sup> New Space Economy, “Understanding the Ethical Landscape of the Space Economy,” Understanding the Ethical Landscape of the Space Economy, August 27, 2023, <https://newspaceeconomy.ca/2023/08/27/understanding-the-ethical-landscape-of-the-space-economy/>.

<sup>26</sup> Plotnek and Slay, p.253.

<sup>27</sup> Steer, p.10.

<sup>28</sup> Erickson & Azcárate Ortega, “To Space Security and Beyond,” (2023).

<sup>29</sup> Zahoor, p.122.

weapons or counter space capabilities located in or directed towards space or space systems.”<sup>30</sup> This aspect of space activity introduces the concept of space threats, intentional human activities causing damage or risk for space systems. One important aspect of this is the anti-satellite technologies (ASATs) specifically “designed to destroy or limit satellites for military purposes.”<sup>31</sup> The discussions surrounding ASATs is elusive since a spacecraft not intended for counter space activities, such as repair satellites, can be repurposed for counter space activities, simply by ramming into other satellites.<sup>32</sup> Hence, in discussing space threats, intentionality is a key aspect.

---

## Space Threats

UNIDIR defines space threats as “the possibility of intended or intentional damage (involving agency, or done in a deliberate manner) to space systems.”<sup>33</sup> Threats to space systems can be categorized in several ways, based on threat vectors, Earth-to-Earth, Space-to-Space, Earth-to-Space and Space-to-Earth, or on different categories of space threats, such as kinetic, electromagnetic, political and cyber,<sup>34</sup> or based on operational segments, the ground, the space and the link connecting the two.<sup>35</sup> To better visualise the various operating principles of space threats, this paper follows the categorization based on threat vectors. However, the threat vectors are insufficient to capture the whole range of threats constituted by intentional human actions concerning space, because of which this categorization is supplemented by the categories “political threats” and the “cyber threats”, which operate both outside and through all threat

---

<sup>30</sup> Erin Pobjie and Almudena Azcárate Ortega, “Space Security Legal Primer 1- Outer Space & Use of Force,” UNIDIR, September 2024, p.11.

[https://unidir.org/wp-content/uploads/2024/09/UNIDIR\\_Outer\\_Space\\_and\\_Use\\_of\\_Force.pdf](https://unidir.org/wp-content/uploads/2024/09/UNIDIR_Outer_Space_and_Use_of_Force.pdf).

<sup>31</sup> Talia Blatt, “ANTI-SATELLITE WEAPONS AND THE EMERGING SPACE ARMS RACE,” Harvard *International Review* 41, no. 3 (2020), Gale Academic OneFile, p.30,

<https://link.gale.com/apps/doc/A699459154/AONE?u=hei&sid=bookmark-AONE&xid=0db5af02>.

<sup>32</sup> Blatt, p.30.

<sup>33</sup> Azcárate Ortega, Almudena and Victoria Samson (Eds.). “A Lexicon for Outer Space Security.” UNIDIR. Geneva. August 16th, 2023, p.41,

[https://unidir.org/wp-content/uploads/2023/09/UNIDIR\\_Lexicon\\_for\\_Outer\\_Space\\_Security.pdf](https://unidir.org/wp-content/uploads/2023/09/UNIDIR_Lexicon_for_Outer_Space_Security.pdf).

<sup>34</sup> UNIDIR, “Threats to the security of space activities and systems,” Open-ended working group on reducing space threats through norms, rules and principles of responsible behaviours, A/AC.294/2022/WP.16, September 12th, 2022, United Nations General Assembly, p.4-5,

[https://documents.un.org/symbol-explorer?s=A/AC.294/2022/WP.16&i=A/AC.294/2022/WP.16\\_3739988](https://documents.un.org/symbol-explorer?s=A/AC.294/2022/WP.16&i=A/AC.294/2022/WP.16_3739988).

<sup>35</sup> Varadharajan, Vijay, and Neeraj Suri. *Security challenges when space merges with Cyberspace*, 2023, 1.

vectors.

Hence, space threats include: (i) Political Threats; (ii) Ground-to-Space Threats; (iii) Space-to-Ground Threats; (iv) Space-to-Space Threats; (v) Ground-to-Ground Threats; and (vi) Cyber Threats.

## **(i) Political Threats**

### **a) Geopolitical Context**

While Space has never not been a site of geopolitics, there has been a shift in its intensity.<sup>36</sup> This intensity does not occur without context. It reflects territorial politics that have intensified the development of what scholars call *astro-geopolitics*. The concept of geopolitical tensions might not constitute a threat in itself, but it produces several challenges, problems, and incidents that arguably become a threat to the idea of Space Security. A threat does not exist without a context. As Victoria Samson notes, "space is a lagging indicator for politics on Earth".<sup>37</sup>

The intensification of Space and its uses, is not limited to the Global North, but a trend that can be seen across the globe. In Africa, 20 countries now have space programs, with thirteen States owning space agencies. Additionally, the African Union has made space expansion a point on Agenda 2063.<sup>38</sup> Several heads of State on the continent emphasized the need for "continental growth by enhancing capabilities in Earth observation, navigation, positioning systems, satellite communication, and space exploration."<sup>39</sup>

Prominent world leaders further characterize the geopolitical tensions in several speeches. French President Emmanuel Macron gave a speech in Toulouse, telling the crowd that Space is the new frontier, Russian President Vladimir Putin states that "Russia's undisputed leadership" in the

---

<sup>36</sup> Elefteriu Fraes, "The Role of Space Power in Geopolitical Competition.", p. 4.

<sup>37</sup> Samson, "The Geopolitics of a New Modern Space Race," 2021, <https://www.institutmontaigne.org/en/expressions/geopolitics-new-modern-space-race>.

<sup>38</sup> Ngcofe, "Is There Enough Space for Africa in Outer Space?", p.2.

<sup>39</sup> Ibid.

Space area must continue to grow."<sup>40</sup> The African Union, in its Agenda for Africa for 2063, aspires that Africa will have its rightful share of the global commons of land, oceans, and Space.<sup>41</sup>

The militarization of Space is not a new concept, it has had a substantial impact on the global military balance and is increasingly relied on for communications, strikes and other military use.<sup>42</sup>

Space and Space-access does not always have to be for military use, Space power theory describes it as a tool of indirect and soft power or as a directly strategic, but non-military.<sup>43</sup> Satellite imagery can be used by States as a tool of collecting data, such as verifying carbon emissions and addressing other types of socioeconomic challenges.<sup>44</sup> This is especially the case for developing States, where it can play an important part in addressing socioeconomic and security threats.<sup>45</sup> It can serve as a symbol or tool of national power, with China and Arab States developing a "Space Silk Road".<sup>46</sup> Additionally, Space can be used as a tool for development, it can aid in predicting crop failure, measuring deforestation, and desertification.<sup>47</sup>

Russia has narrowed their focus to counter space capabilities, while China's rapidly advancing space program is projected to "erode American influence across military, economic, and diplomatic spheres" by 2030.<sup>48</sup> In India, there has been an increasing amount of security challenges due to the developments of their neighbors. Hence, India has outlined an aim to develop their self-reliance in Space, in order to meet geopolitical crises that might occur.<sup>49</sup>

When speaking to several interviewees, multiple shared the view that due to the current geopolitical climate, there is the impression that multilateral discussions about space security are

---

<sup>40</sup> Macron, "Prononcé Le 11 Décembre 2023 - Emmanuel Macron 11122023 Plan France 2030 | Vie-Publique.Fr.", Putin, "Meeting on Development of Space Activities."

<sup>41</sup> The African Union, *Agenda 2063*, p. 10.

<sup>42</sup> Elefteriu Fraes, "The Role of Space Power in Geopolitical Competition.", p. 4.

<sup>43</sup> Ibid.

<sup>44</sup> Ibid.

<sup>45</sup> Garrido Guijarro, "A Common African Outer Space Policy to Meet the Continent's Challenges."

<sup>46</sup> Ming, "The Space Silk Road and China–Arab States Space Cooperation."

<sup>47</sup> Elefteriu Fraes, "The Role of Space Power in Geopolitical Competition."

<sup>48</sup> Ibid.

<sup>49</sup> Chandrashekar, "India and the Peaceful Uses of Outer Space." p. 449.

becoming increasingly stagnant.<sup>50</sup> The increase of geopolitical tensions limits international cooperation, and rather than becoming a priority, it becomes a subordinate concern that relies on a political objective agenda. This has made it "impossible to gain momentum for international coordination."<sup>51</sup> It was further stated by another interviewee the role of international law and types of soft law mechanisms will be ineffective unless they are backed by what they called a genuine political commitment and that "if no one is committed to keep the rules, then those rules are just a piece of paper."<sup>52</sup>

What is the role of internationalism in space security? In one interview, they argued that the United Nations is the most appropriate body to bring forth the discussion on the rules of maintaining space security but remained hesitant on the possibility of any agreement between the major dominant space powers, because there is a limited area of consensus.<sup>53</sup> Simultaneously, Yongliang Yan argues that the current international framework is insufficient in addressing the current geopolitical challenges.<sup>54</sup> Instead, they argue that it would be more efficient to regionalize these topics for more effective governance. Mabuni and Manatan argue that any significant progress towards international cooperation might not be possible in the near-term future due to the geopolitical conditions.<sup>55</sup> They also highlight the role of regional cooperation, specifically in the Asia-Pacific region.<sup>56</sup>

Hence, it can be understood that the current geopolitical tension is a risk to Space security, as it is a contributing factor to the erosion of trust, the continued militarization of Outer Space and the stalling international cooperation.

---

<sup>50</sup> Interview Data.

<sup>51</sup> Ibid.

<sup>52</sup> Ibid.

<sup>53</sup> Ibid.

<sup>54</sup> Yan, "Capacity Building in Regional Space Cooperation." no page number.

<sup>55</sup> Mabuni and Manantan, "Accelerating Asia-Pacific Space Economies Through Regional Partnerships." p.3

<sup>56</sup> Ibid.

## **b) States' Interpretation of "Threat" Concept in the Context of Space Law**

The characterization of a "threat" in international law is complex and different from culture to culture. While treaties such as the Outer Space Treaty and the Liability Convention establish baseline norms, such as peaceful purpose, non-appropriation and non-interference, international liability<sup>57</sup> and fault-based liability,<sup>58</sup> the specification of a threat cannot be universalized, but rather highly contextualized to legal, linguistic, and geopolitical contexts. In space law, a threat is expansive; it could include the placement of weapons in orbit, satellite collision, and the threat of cyberattack aimed at the infrastructure of space systems. This broad definition also illustrates the need to analyze State declarations, the role of language in legal significance, the implications for international relations and security.<sup>59</sup>

In order to explore what "threat" means in space law, it is first useful to explore a broader understanding of threat in discourses within national legal and strategic contexts. Generally, in security contexts threat refers to both intent and capability for harm. However, States tend to interpret the intent-capacity construct differently. This section will look at how major space-faring States interpret "threat" in terms of space activities based on a comparative analysis of their legal and strategic policies. The comparative study of national legal and strategic inquiries goes further in demonstrating the issues of reaching consensus on threats in law.

### **1. United States: Intent and Capability.**

In the landscape of law in the U.S., a "threat" needs to be understood in terms of intentionality and capability. Although the U.S. law has not offered an outright definition of "threat" that universally combines both intent and capability across all contexts, laws and official documents suggest this understanding. The National Security Act of 1947,<sup>60</sup> for example describes "foreign

---

<sup>57</sup> Articles II, IV, VI and IX of the Outer Space Treaty (1967).

<sup>58</sup> Article III of the Liability Convention.

<sup>59</sup> United Nations, "*Threats to the security of space activities and systems*," Submitted by the United Nations Institute for Disarmament Research (UNIDIR).

[https://documents.unoda.org/wp-content/uploads/2022/08/20220817\\_A\\_AC294\\_2022\\_WP16\\_E\\_UNIDIR.pdf](https://documents.unoda.org/wp-content/uploads/2022/08/20220817_A_AC294_2022_WP16_E_UNIDIR.pdf)

<sup>60</sup> United States. U.S. Code Title 50 – War and National Defense, Section 3003: Definitions. Accessed April 11, 2025.

<https://uscode.house.gov/view.xhtml?edition=prelim&num=0&req=granuleid%3AUSC-prelim-title50-section3003>.

intelligence” as information in respect to the “capabilities, intentions, or activities” of foreign agents. A “threat,” especially in areas of national security, is understood as a potential enemy as someone with intent and the capability of taking an action.<sup>61</sup>

As with other treaties, the United States views international space agreements through the lens of national security, focusing on threat assessment involving the intent and capability of other potential hostile actors. This is exemplified in the Space Policy Directive--5 (2020)<sup>62</sup> where it features risks perceived critical such as cyber vulnerabilities to space systems. Support for this policy interpretation exists in academic literature<sup>63</sup> which argues that U.S. space policy responds to space as a contested domain where adversary capabilities and intentions must be counteracted.

## 2. Russia: Strategic Stability and Political Narrative.

In Russian strategy and diplomacy, the Russian word “угроза”<sup>64</sup> (threat) is much broader than the word threat in English, encompassing military aggression and foreign policy strategy, but also technology development that is viewed as subversively detrimental. This reflects a geopolitical orientation where threats are perceived as measures that are designed to destroy the threats to Russia’s sovereignty, even in their internal order. In respect to space law, Russia has always said that the militarisation of space, especially with the building of missile defence systems, threatens space.<sup>65</sup>

In the framework of space law, Russia is forever resisting the militarisation of outer space and considers space weapons, and missile defence systems, a threat to strategic stability.<sup>66</sup> In the

---

<sup>61</sup> Center for Development of Security Excellence (CDSE), “Risk Management for DoD Security Programs Training Glossary,” <https://www.cdse.edu/Portals/124/Documents/glossary/GS102-glossary.pdf>.

<sup>62</sup> White House. Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems. September 4, 2020.

<https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/>.

<sup>63</sup> Shmigol, Valerie. “The United States Is Enabling an Outer Space Arms Race: An Overview of the Current Framework and Recommendations for Abating an Outer Space Arms Race.” *Seattle University Law Review* 46, no. 1 (2022): 175–200. <https://digitalcommons.law.seattleu.edu/sulr/vol46/iss1/7/>.

<sup>64</sup> AI was used to generate this word.

<sup>65</sup> The Ministry of Foreign Affairs of the Russian Federation. Statement by the Representative of the Delegation of the Russian Federation at the Thematic Discussion on “Outer Space (Disarmament Aspects)” in the First Committee of the 79th session of the UN General Assembly, New York, October 29, 2024.

[https://mid.ru/en/foreign\\_policy/news/1978174/?TSPD\\_101\\_R0=08765fb817ab2000e5de439d1c79638a2203927a352bc12e32f12659d1c00b35a1f57d65880c8b9d080f95f249143000d1d2f7561529d8bdc8ab85835fb1e6ede76b476022d0054bc4c597018f0ef0c8dccc6794ffe113d380049da3dd065d3f5](https://mid.ru/en/foreign_policy/news/1978174/?TSPD_101_R0=08765fb817ab2000e5de439d1c79638a2203927a352bc12e32f12659d1c00b35a1f57d65880c8b9d080f95f249143000d1d2f7561529d8bdc8ab85835fb1e6ede76b476022d0054bc4c597018f0ef0c8dccc6794ffe113d380049da3dd065d3f5).

<sup>66</sup> Center for Strategic and International Studies (CSIS), “Space Threat Assessment 2021”. [https://aerospace.csis.org/wp-content/uploads/2021/03/CSIS\\_Harrison\\_SpaceThreatAssessment2021.pdf](https://aerospace.csis.org/wp-content/uploads/2021/03/CSIS_Harrison_SpaceThreatAssessment2021.pdf).

domestic Russian perception, “threat” loses its neutral legal connotation in the sense of an empty vessel waiting to be filled with contents, but becomes an instrument of political and ideological tool intended to consolidate the national narrative of defensive against external hybrid war offensives.

Russia’s official foreign policy positions the country as constantly besieged by Western influence operations designed to dismantle its political system and erase its cultural identity.<sup>67</sup> Russia views international space treaties from a geopolitical and security perspective, where the concept of “threat” (угроза) involves direct military hostilities and policies or technologies that are deemed strategically harmful. This is one of the guiding ideas of the Foreign Policy Concept of the Russian Federation (2023),<sup>68</sup> which underlines the need to guard sovereignty, territorial integrity, and national interests from ruinous external forces.

### 3. China: Sovereignty and Autonomy.

China’s perception of “threat” is heavily related to its principles of sovereignty and non-interference. The Chinese State has employed the legal and diplomatic dual use of the term “威胁”<sup>69</sup> (wēixié), which means direct military threats or indirect challenges to national interests such as economic and technological warfare.<sup>70</sup>

China interprets space treaties with profoundly defensive and sovereignty focused attitudes: anything that threatens strategic autonomy or enables the projection of foreign powers into China’s sphere of influence – be it direct or indirect. This causes China to create softer but still restrictive legal instruments, reject western unilateral treaties, and promote the development of self-sufficient, deterrent space capabilities. China states that all countries have equal rights to the peaceful exploration, development and use of outer space. China also embraces the idea of a community of shared destiny by claiming cooperation based on equality and mutual benefits.<sup>71</sup>

---

<sup>67</sup> Pynnöniemi, K., & Jokela, M. (2020). Perceptions of hybrid war in Russia: means, targets and objectives identified in the Russian debate. *Cambridge Review of International Affairs*, 33(6), 828–845. <https://www.tandfonline.com/doi/full/10.1080/09557571.2020.1787949>.

<sup>68</sup> Ministry of Foreign Affairs of the Russian Federation. The Foreign Policy Concept of the Russian Federation. March 31, 2023. [https://mid.ru/en/foreign\\_policy/fundamental\\_documents/1860586/](https://mid.ru/en/foreign_policy/fundamental_documents/1860586/).

<sup>69</sup> AI was used to generate this word.

<sup>70</sup> The State Council Information Office of the People’s Republic of China. “China’s National Defense in the New Era,” Center for Strategic and International Studies, <https://www.csis.org/analysis/chinas-new-2019-defense-white-paper>.

<sup>71</sup> The State Council. The Peoples Republic of China. “China’s Space Program: A 2021 Perspective.”

#### 4. The European Union: Risk Management and Multilateralism.

The European Union’s definition of “threat” emphasizes prevention and proactive management and mitigating processes in a risk management framework.<sup>72</sup> While the EU recognizes the need to consider direct malicious acts of violence, they generally categorize hostile actions as “potential risks,” distinguishing between things that were attempts to cause harm and the acts of hostile assertiveness that were not intended to cause harm, even including the placement of counter space capable systems.

The EU understands international space treaties as not legal limits but as necessary structures to be harmonized through sustained engagement, multilateralism and regulating in an anticipatory manner. The EU promotes peaceful uses of outer space and supports non-binding initiatives such as soft law instruments, technical norms and policy (policy mandates) towards sustainability in the outer space<sup>73</sup>, which is qualified by the EU as a global commons space and emphasizes the UN as a critical governance structure with expressions of sovereign equality and environmental safeguard principles.<sup>74</sup>

#### 5. Japan: Existential Risk.

In the context of Japanese security discourse, the term 脅威<sup>75</sup> (kyōi) is often aligned with the English “threat.” As part of our research, we interviewed a Japanese academic. He describes threat as a harmful greater power or force which endangers the existence of an individual or a nation and is a fact of life that must be managed and avoided.

Also, the academic believes that kyōi for Japan can be alleviated through reduced exposure risk and outside affiliations, like the alliance with the United States. Within the structure, any act of aggression, including the assault on Japanese space assets, is considered an infringement of Japanese domain and as such, may be interpreted as an attack on national territory and therefore fall under the protections of Article 5 of the Japan-U.S. Security Treaty, which closely mirrors

---

[https://english.www.gov.cn/archive/whitepaper/202201/28/content\\_WS61f35b3dc6d09c94e48a467a.html](https://english.www.gov.cn/archive/whitepaper/202201/28/content_WS61f35b3dc6d09c94e48a467a.html).

<sup>72</sup> European Parliament. “EU space strategy for security and defence.” (2023)

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754598/EPRS\\_BRI%282023%29754598\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754598/EPRS_BRI%282023%29754598_EN.pdf).

<sup>73</sup> Frans G. von der Dunk. “The European Union and the Outer Space Treaty: Will the Twain Ever Meet?”

<https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1089&context=spacelaw>.

<sup>74</sup> Larik, J. (2023). EU law and the governance of Global Spaces: ambitions, constraints and legal creativity. *Journal of European Integration*, 45(8), 1125–1142. <https://www.tandfonline.com/doi/full/10.1080/07036337.2023.2270670>.

<sup>75</sup> AI was used to generate this word.

Article 5 of the NATO Charter.

## **(ii) Ground-to-Space Threats**

Ground-to-Space threats are based on the Earth, but pose a threat to space objects when launched into space.<sup>76</sup> Ground-to-Space threats include: a) direct-ascent ASATs such as ballistic missiles launched from the Earth; as well as b) ground-based directed energy weapons such as lasers and high powered microwave systems.

ASAT development and testing began in the Cold War as the United States and the Soviet Union sought “means of countering each other’s capabilities in space.”<sup>77</sup> The United States and the Soviet Union first started their ASAT tests in the 1950s and 1960s, seeking to counter the perceived threat of the other State’s space capabilities.<sup>78</sup>

### **a) Direct-ascent missiles**

An example of ground-based ASATs is that of direct-ascent missiles launched from the Earth, such as ballistic missiles. Direct-ascent missiles (including ballistic missiles) are weapons which can directly hit a space object in low earth orbit (with an altitude of up to 2000 kilometres or 1200 miles) or detonate a warhead near it.<sup>79</sup> Kinetic anti-satellite tests using direct-ascent missiles have already been conducted by four States to destroy their own satellites: the United States, China, Russia, and India.<sup>80</sup>

In chronological order of their first test: the first instance where the United States of America’s destroyed its own satellite in a direct-ascent ASAT test was in September 1985,<sup>81</sup> and its most

---

<sup>76</sup> Blatt, p.30.

<sup>77</sup> Laura Grego, “Security in Space: What Is at Stake and How Do We Move Forward?” *Asian Perspective* 35, no. 4 (2011): p.511. <http://www.jstor.org/stable/42704769>.

<sup>78</sup> Laura Grego, “A History of Anti-Satellite Programs,” Union of Concerned Scientists, January 2012, p.2, [https://www.ucs.org/sites/default/files/2019-09/a-history-of-ASAT-programs\\_lo-res.pdf](https://www.ucs.org/sites/default/files/2019-09/a-history-of-ASAT-programs_lo-res.pdf).

<sup>79</sup> Anelí Bongers and José L. Torres, “Star Wars: Anti-Satellite Weapons and Orbital Debris,” *Defence and Peace Economics* 35, no. 7 (2023): p.830. <https://doi.org/10.1080/10242694.2023.2208020>.

<sup>80</sup> Ibid.

<sup>81</sup> Ibid, p.831.

recent one was in February 2008;<sup>82</sup> China's first direct-ascent ASAT test against its own satellite was conducted in January 2007,<sup>83</sup> and its most recent one was in February 2018,<sup>84</sup> Russia's first direct-ascent ASAT test against its own satellite was conducted in December 2018,<sup>85</sup> while their most recent direct-ascent ASAT test (also the most recent direct-ascent ASAT test in history) was in November 2021,<sup>86</sup> and India's one direct-ascent ASAT test against its own satellite was conducted in 2019.<sup>87</sup> Each of these tests produced debris, ranging from 129 catalogued pieces of debris in India's 2019 test to 3,449 catalogued pieces of debris in China's 2007 test.<sup>88</sup>

Views on direct-ascent ASATs vary. An interviewee drew attention to States pushing to ban ASAT tests of this kind,<sup>89</sup> and another interviewee described how there are States who do wish to develop them.<sup>90</sup> An expert from the Global South described how direct-ascent ASATs are not a priority for States from the Global South to obtain or restrict, instead focusing on more imminent threats like cyberattacks.<sup>91</sup> This expert mentioned that direct-ascent ASATs would only become a priority if more States start to do such tests.<sup>92</sup>

Another direct ascent example is that of existing anti-ballistic missile systems, which could have counter space capabilities."<sup>93</sup> Launched from the ground, anti-ballistic missile systems are already intended to destroy nuclear missiles which travel through outer space at high altitudes, so they therefore have ASAT capabilities.<sup>94</sup>

---

<sup>82</sup> Ibid.

<sup>83</sup> Ibid.

<sup>84</sup> Ibid.

<sup>85</sup> Ibid.

<sup>86</sup> Dimitrios Strokos, "Still Lost in Space? Understanding China and India's Anti-Satellite Tests through an Eclectic Approach," *Astropolitics* 21 vol.2-3 (2023): p.179. <https://doi.org/10.1080/14777622.2023.2277253>.

<sup>87</sup> Daniel Porras, "Anti-Satellite Warfare and the Case for an Alternative Draft Treaty for Space Security," *Bulletin of the Atomic Scientists* 75, no. 4 (2019): p.142. <https://doi.org/10.1080/00963402.2019.1628470>.

<sup>88</sup> Bongers and Torres, p.831.

<sup>89</sup> Interview Data.

<sup>90</sup> Ibid.

<sup>91</sup> Ibid.

<sup>92</sup> Ibid.

<sup>93</sup> Thomas Markram, "Possible Challenges to Space Security and Sustainability," *Arms Control Today* 47, no. 10 (2017): p.44, <https://www.jstor.org/stable/90016032>.

<sup>94</sup> Victoria Samson and Laetitia Cesari. Secure World Foundation, "Global Counterspace Capabilities Report 2025," April 3rd, 2025, p. 61, [https://swfound.org/media/208099/swf\\_global\\_counterspace\\_capabilities\\_2025.pdf](https://swfound.org/media/208099/swf_global_counterspace_capabilities_2025.pdf).

## **b) Ground-based directed energy weapons**

Ground-based directed energy weapons include lasers which are stationed on the Earth that could target, damage, and destroy satellites through heating.<sup>95</sup> Ground-based lasers can dazzle or blind satellites with a goal to target and overwhelm a satellite's sensors to disrupt its functionality.<sup>96</sup> Dazzling is temporary, and blinding is long-term damage.<sup>97</sup> The use of ground-based lasers was tested by: the United States in 1997 to illuminate a satellite orbiting at an altitude of 420 kilometres (about 261 miles);<sup>98</sup> China in 2005 against a low earth orbit satellite at an altitude of 600 kilometres (about 373 miles).<sup>99</sup> Ground-based High Powered Microwave (HPM) systems, meanwhile, are another form of directed energy weapons that can be used to disrupt and damage the electronics of a satellite using electromagnetic waves.<sup>100</sup> These may not be very feasible as they would need a very high level of power over a long distance, and a large antenna to do so.<sup>101</sup>

## **(iii) Space-to-Ground Threats**

Space-to-Ground threats are based in space but pose a threat to the Earth.<sup>102</sup> They could be directed at the Earth, or disruption and damage to space segments of space systems can have impacts on the ground. Space-to-Ground threats include: a) nuclear detonation in space (even though this is prohibited); b) space-based directed energy weapons such as lasers; and c) kinetic bombardment, or dropping objects from space onto the Earth.

---

<sup>95</sup> Steve Fetter, "Protecting our Military Space Systems" in Edmund S. Muskie, ed., *The U.S. in Space: Issues and Policy Choices for a New Era* (Washington DC: Center for National Policy Press, 1988), p.6, <https://cisssm.umd.edu/sites/default/files/2019-08/1988-CNP-ASAT.pdf>.

<sup>96</sup> Max M. Mutschler, "The Danger of an Arms Race in Space," *Keeping Space Safe: Towards a Long-Term Strategy to Arms Control in Space*, Peace Research Institute Frankfurt, January 1st, 2010, p.4, <http://www.jstor.org/stable/resrep14496.4>.

<sup>97</sup> Samson and Cesari, p. 80.

<sup>98</sup> Grego, "A History of Anti-Satellite Programs," p.7.

<sup>99</sup> Ibid, p.163.

<sup>100</sup> Mutschler, p.4.

<sup>101</sup> David Wright, Laura Grego, and Lisbeth Gronlund, "The Physics of Space Security: A Reference Manual," American Academy of Arts & Sciences, 2005, p. 131. <https://aerospace.csis.org/wp-content/uploads/2019/06/physics-space-security.pdf>.

<sup>102</sup> Todd Harrison, "Framework for Evaluating Space Weapons," in *International Perspectives on Space Weapons*, Center for Strategic and International Studies (CSIS), 2020, p. 8, <http://www.jstor.org/stable/resrep24829.6>.

### a) Nuclear detonation from space

Nuclear detonations in space pose a threat to the Earth, even though it is prohibited. The Soviet Union and the United States both tested nuclear weapons in space at least nine times during the years 1957-1962.<sup>103</sup> Following this were the drafting of Treaties seeking to ban nuclear testing in space, such as the 1963 *Partial Test Ban Treaty* and the 1967 *Outer Space Treaty*.<sup>104</sup> With the former, Article I prohibited nuclear test explosions in the atmosphere and in outer space.<sup>105</sup> With the latter, Article IV prohibited the placement of weapons of mass destruction into orbit and on celestial bodies.<sup>106</sup>

One of the ways in which nuclear detonations in space are a threat to the Earth is that they can cause an Electromagnetic Pulse (EMP), which are sources of electrical and magnetic energy that can damage or disable electronic equipment and electric equipment.<sup>107</sup> When a nuclear weapon is detonated at a high altitude, it can destroy satellites near it,<sup>108</sup> but it also has many impacts on the ground. This was the case in the ‘Starfish Prime’ nuclear test. Starfish Prime was a high-altitude nuclear test conducted by the United States on the 9th of July, 1962.<sup>109</sup> 400 kilometres (250 miles) above the Johnston Atoll, the bomb was detonated, and over 1280 kilometres (800 miles) away street lights went out in Oahu, Hawaii as the bomb went off.<sup>110</sup> Similarly in the K-3 high-altitude nuclear explosion in the Soviet Union on the 22nd of October, 1962, there were impacts on the ground.<sup>111</sup> The EMP caused an Air Defense radar to fail, an underground power cable was disabled, power generators were rendered out of service, and there were fires due to

---

<sup>103</sup> Moltz, p.188.

<sup>104</sup> Ibid, p.189.

<sup>105</sup> The Union of Soviet Socialist Republics, the United Kingdom of Great Britain and Northern Ireland and the United States of America, “Treaty banning nuclear weapon tests in the atmosphere, in outer space and under water,” 15th October 1963, <https://treaties.un.org/doc/Publication/UNTS/Volume%20480/volume-480-I-6964-English.pdf>.

<sup>106</sup> United Nations General Assembly. Article IV of the “Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies.” December 19th, 1966. Resolution 2222 (XXI). [https://www.unoosa.org/pdf/gares/ARES\\_21\\_2222E.pdf](https://www.unoosa.org/pdf/gares/ARES_21_2222E.pdf).

<sup>107</sup> David Ochmanek and Lowell H. Schwartz, “The Uniquely Destructive Capabilities of Nuclear Weapons,” in *The Challenge of Nuclear-Armed Regional Adversaries*, 1st ed., RAND Corporation, 2008, p.8, <http://www.jstor.org/stable/10.7249/mg671af.10>.

<sup>108</sup> Wright, Grego, and Gronlund, p.17.

<sup>109</sup> Charles N. Vittitoe, “Did High-Altitude EMP Cause the Hawaiian Streetlight Incident?” Sandia National Laboratories, June 1989, p.3, <https://ece-research.unm.edu/summa/notes/SDAN/0031.pdf>.

<sup>110</sup> Ibid.

<sup>111</sup> Vladimir Gurevich, “New Strategy is Needed to Solve the 50-Year-Old Problem - EMP Protection of Critical Civilian Infrastructure,” *International Journal of Emerging Science and Engineering* 12, no. 2: January 2024, p.6, <https://www.ijese.org/wp-content/uploads/Papers/v12i2/L25571111223.pdf>.

the short-circuiting of electric appliances.<sup>112</sup>

### **b) Space-based directed energy weapons**

Space-based directed energy weapons are stationed in space, and can be aimed at the Earth. Space-based lasers could, in principle, target objects in the air, such as aircraft in-flight, or on the surface.<sup>113</sup> They could also be used to intercept missiles, which was considered by the United States under the Presidency of Ronald Reagan (under the Strategic Defense Initiative, nicknamed as “Star Wars”).<sup>114</sup> The feasibility of space-based directed energy weapons is difficult, however, as there could be atmospheric limitations for the laser light (which would already need to be at a very high power) meaning laser light could be disturbed by turbulence, water vapour, weather, and other aerosols.<sup>115</sup>

### **c) Kinetic bombardment**

Kinetic bombardment is the concept that a conventional weapon could be carried into space and when dropped on command, use its high speed to destroy a target on the Earth.<sup>116</sup> An example of this is the “Rods from God” concept where tungsten rods would be dropped on the Earth.<sup>117</sup> This could create damage equivalent to the use of a small nuclear weapon. The feasibility of kinetic bombardment is difficult, however, because there would be a need for the conventional weapon to be able to withstand intense heat when it re-enters the atmosphere.<sup>118</sup>

## **(iv) Space-to-Space Threats**

Space-to-Space threats are threats which are based in space and pose a threat to other space objects. These threats can be both apparent and latent, as it is difficult to ascertain the intentions of space powers due to the dual-purpose nature of space assets, which introduces a security

---

<sup>112</sup> Ibid.

<sup>113</sup> Harrison, “Framework,” p.6.

<sup>114</sup> Mutschler, p.6.

<sup>115</sup> Wright, Grego, and Gronlund, p.123.

<sup>116</sup> Harrison, “Framework,” p.6.

<sup>117</sup> Ibid, p. 8.

<sup>118</sup> Wright, Grego, and Gronlund, p.59-60.

dilemma for the physical protection of assets in space.<sup>119</sup> Instead, the utilization of space objects with malignant intent provides significant strategic advantages for offense in space. The inability to ascertain intentions enable attacks to be instantaneous, impossible to intercept or prevent and make it easy to coordinate a multiplicity of attacks simultaneously, while direct ascent weapons take time from launch to impact and hence are avoidable.<sup>120</sup> This is also exacerbated by the fact that the deployment of weapons in space, except the weapons of mass destruction, is not forbidden by international law.<sup>121</sup>

In simple terms, space-to-space threats include space-based weapons, also known as co-orbital ASATs, and dual-purpose objects, such as satellites with physical interference capabilities, satellites with rendezvous and proximity operations (RPO) capabilities and satellites with laser capabilities. The threats in this domain are underlined with a general lack of legal framework for the aversion of such threats.

#### **a) Co-Orbital ASATs**

Co-orbital ASATs are interceptors which are placed into orbit and manoeuvred to their targets. They can collide with their targets, detonate near them, release projectiles towards them, or use a robotic arm to damage them.<sup>122</sup> Releasing projectiles can include shrapnel (specifically, a cloud of pellets) which is directed towards the path of other space objects with the intent to damage them.<sup>123</sup> Co-orbital ASATs can remain dormant until triggered, making them difficult to identify as weapons and especially so if they are being used for peaceful space operations.<sup>124</sup> For example, a State could announce the deployment of a satellite, but not that a co-orbital ASAT is on the same launcher for it.<sup>125</sup> Not only are they hard to detect, but they are cheaper and more accessible than major satellites- this means that States who are emerging space powers can develop them against larger space powers.<sup>126</sup>

---

<sup>119</sup> Yoon and Um, 344

<sup>120</sup> Chow, 84

<sup>121</sup> Poirier, 2

<sup>122</sup> UNIDIR, "Threats to the security of space activities and systems," p.4.

<sup>123</sup> Mutschler, p.5.

<sup>124</sup> Cottam, "How to Prevent a War in Space (Part 1).

<sup>125</sup> Grego, p.153.

<sup>126</sup> Mutschler, p.5.

The first successful co-orbital ASAT test was conducted by the Soviet Union in October of 1968, where the Cosmos 252 satellite exploded and destroyed Cosmos 248.<sup>127</sup> The United States followed in September 1986 where a Delta 2 rocket was made to collide with a Payload Assist System platform with a warhead.<sup>128</sup> China conducted its first test in June 2010, with the SJ-12 satellite causing the SJ-6F satellite to move away from its orbital position.<sup>129</sup> The development and/or testing of co-orbital ASATs is a concern to States like Brazil, who made a submission to the Open-Ended Working Group (OEWG) on Reducing Space Threats Through Norms, Rules and Principles of Responsible Behaviours. Brazil highlighted that the debris this causes can impact the costs of launching and operating space assets, with a specific negative impact on developing States and States with fewer space objects.<sup>130</sup>

## **b) Dual-Purpose Objects**

Dual-purpose objects are space objects which are designated for benign purposes, but which can also be used for damaging or destroying space objects.<sup>131</sup> Satellites deployed for various purposes, like Active Debris Removal, on-orbit servicing, remote sensing, etc. can also be used to disrupt, degrade or destroy other satellites.<sup>132</sup> This nature of space objects makes it hard to define the term “space weapons”<sup>133</sup> and makes it hard to assess to what extent space is weaponized.<sup>134</sup> Hence, maneuvers of space objects can be interpreted as offensive activities in the absence of notification.<sup>135</sup>

---

<sup>127</sup> Bongers and Torres, p.832.

<sup>128</sup> Victoria Samson, “Fact sheet: U.S. Co-Orbital Anti-Satellite Testing,” Secure World Foundation, December 2024, p.2, [https://swfound.org/media/207999/fs24-07\\_us-co-orbital-anti-satellite-testing.pdf](https://swfound.org/media/207999/fs24-07_us-co-orbital-anti-satellite-testing.pdf).

<sup>129</sup> Bongers and Torres, p.832.

<sup>130</sup> Delegation of Brazil, “Destructive Anti-satellite Weapons,” Open-ended working group on reducing space threats through norms, rules and principles of responsible behaviours, A/AC.294/2023/WP.13, February 6th, 2023, United Nations General Assembly, p.1. [https://documents.un.org/symbol-explorer?s=A/AC.294/2022/WP.16&i=A/AC.294/2022/WP.16\\_3739988](https://documents.un.org/symbol-explorer?s=A/AC.294/2022/WP.16&i=A/AC.294/2022/WP.16_3739988).

<sup>131</sup> Steer, p.12.

<sup>132</sup> Cerny et al, 38; Blatt, p.30.

<sup>133</sup> Cesar Jaramillo. “The Multifaceted Nature of Space Security Challenges.” Space Policy 33 (August 2015): p.64-65 <https://doi.org/10.1016/j.spacepol.2015.02.007>; Rathgeber and Remuss, p. 65.

<sup>134</sup> Pepperkamp, 48

<sup>135</sup> Wu, 22

Prior to engaging the various examples of dual-purpose objects, it is important to make a distinction between the terms dual-use and dual-purpose. Dual-use denotes the fact that space objects have both military and civilian uses, such as satellites used for navigation purposes.<sup>136</sup>

*Satellites with physical interference capabilities.*

Satellites can be designed to conduct physical alterations on objects and bodies in space, through the use of robotic arms, projectiles and similar tools. Technology aimed at removing defunct satellites or other space junk, called Active Debris Removal (ADR), which utilizes technology such as robotic arms, can also remove and dismantle active satellites.<sup>137</sup> On-orbit servicing (OOS) spacecraft, designed to conduct maintenance and repair operations on active satellites, also has dual-purpose capabilities, since it can use nets, harpoons, magnets, or robotic arms to refuel and repair satellites.<sup>138</sup> Another emerging capability is satellites capable of asteroid mining, equipped with Small Carry-on Impactors that shoot projectiles to collect samples, which when used against a satellite instead of an asteroid can function as a co-orbital ASAT.<sup>139</sup>

*Satellites with Rendezvous and Proximity Operation (RPO) capabilities*

There is a lack of consensus on what constitutes an RPO<sup>140</sup>. In general, it refers to two or more satellites approaching one another for contact (rendezvous) or to remain in each other's vicinity to accomplish an objective (proximity).<sup>141</sup> Satellites with RPO capabilities are mostly those with ADR and OOS capabilities,<sup>142</sup> they can be deployed in orbit in peacetime and perform attacks during a crisis.<sup>143</sup> As a result of such a dilemma, some states have begun trials of "bodyguard" satellites, further fueling the security dilemma.<sup>144</sup>

This issue will become more prevalent as the number of satellites with RPO capabilities increases, and it will further increase as repairing active satellites becomes more cost-effective

---

<sup>136</sup> Azcárate Ortega and Samson, p.37-38.

<sup>137</sup> Bongers and Torres, p.827.

<sup>138</sup> António Guterres, "Reducing space threats through norms, rules and principles of responsible behaviours: Report of the Secretary-General," July 13th, 2021, United Nations General Assembly, 76th session, p.97, [https://documents.un.org/symbol-explorer?s=A/76/77&i=A/76/77\\_3095022](https://documents.un.org/symbol-explorer?s=A/76/77&i=A/76/77_3095022).

<sup>139</sup> Krishnan and Vijayakumar, 469

<sup>140</sup> Johnson, Kaitlyn. "Rendezvous and Proximity Operations." *Key Governance Issues in Space*. Center for Strategic and International Studies (CSIS), 2020. <http://www.jstor.org/stable/resrep26047.7>, p. 18.

<sup>141</sup> Azcárate Ortega and Samson, 22-23

<sup>142</sup> Johnson, 2020; 18

<sup>143</sup> Chow, 82

<sup>144</sup> Johnson, 2020; 19

then replacing them<sup>145</sup> and with the emergence of more technological space objects, such as highly maneuverable “space planes.”<sup>146</sup> A number of proposals suggest implementing exclusion zones around satellites, zones which when breached without permission would justify a forceful response.<sup>147</sup> Such proposals showed the technical standards established by the International Space Station, which has special protocols regulating approaching satellites.<sup>148</sup> However, debates around such suggestions concern their legality, especially whether or not they violate OST, which prohibits the appropriation of any section of space.<sup>149</sup>

The lack of a common definition and standards of “normal” RPO behavior emerges as the main challenge of overcoming paranoia for such satellites.<sup>150</sup> The main obstacle in the establishment of standards is, in turn, the lack of national recognition of this issue in the first place as the debates between states on this regard focus on the defensive and offensive implications of RPOs rather than establishing norms and standards of proper RPO behavior.<sup>151</sup>

#### *Satellites with laser capabilities*

Use of laser technology by active satellites provides a multitude of benefits like providing precise up-to-date data for better space traffic management, more precisely locating space debris for removal, enabling larger data transfers, providing solutions for space resource utilization, planetary defense, interstellar travel, etc.<sup>152</sup> Although the laser capabilities satellites can employ are significantly weaker than their ground-based counterparts, they can still temporarily dazzle or blind satellites while permanently damaging certain components.<sup>153</sup>

Moreover, using laser-equipped satellites has certain advantages over ground-based lasers. Such space objects can function as mobile satellite laser ranging units operating in space, hence making surprise attacks and overcoming the laser-protection protocols satellites implement when

---

<sup>145</sup> Ibid, 24

<sup>146</sup> Poirier, 2

<sup>147</sup> Cerny et al, 11

<sup>148</sup> Johnson, 2020; 23

<sup>149</sup> Cerny et al, 15

<sup>150</sup> Johnson, 2020; 23

<sup>151</sup> Ibid, 18-24

<sup>152</sup> Petr Boháček, Topic 3: Current and Future Space-to-Space Threats by States to Space Systems, Agenda Item 6(b), Open-Ended Working Group on Reducing Space Threats Through Norms, Rules and Principles of Responsible Behaviours, Second session, Geneva (14 Sep. 2022).

<sup>153</sup> Ibid, 3

going over known permanent satellite laser ranging stations by tailgating them.<sup>154</sup> Hence, they can instigate an attack at a critical moment to, among other things, blind space-based anti-ballistic sensors.<sup>155</sup> They can also be used to redirect space debris using photon pressure or ablation, which can set them on a collision course with another space object.<sup>156</sup>

### **c) The Sustainable use of Space**

Throughout this research, it has become increasingly clear that Space is an essential part of life on Earth, and we are becoming increasingly reliant on it in order to continue development, this has been acknowledged by the International community, most recently in December 2024, in a United Nations General Assembly (UNGA) resolution that states they are "Convinced that space science and technology and their applications... provide indispensable tools for viable long-term solutions for sustainable development and can contribute more effectively to efforts to promote the development of all countries and regions of the world..."<sup>157</sup>

The concept of sustainability is defined by the United Nations in its Brundtland Commission as the way to ensure that they meet the "needs of the present without compromising the ability of future generations to meet their own needs."<sup>158</sup>

The continued reliance on Space is not limited to development, but it impacts almost all aspects of our lives, from GPS to weather forecasting and access to the Internet. Naturally, this has raised questions on how sustainable the current path is in the long term. Space sustainability has become a concern in international policy and security discussions, particularly as humanity becomes increasingly dependent on space-based infrastructure for navigation, communication,

---

<sup>154</sup> Ibid, 3

<sup>155</sup> Ibid, 4

<sup>156</sup> Ibid, 4

<sup>157</sup> United Nations General Assembly. (2024, December 12). *International cooperation in the peaceful uses of outer space* (A/RES/79/87). United Nations.

<sup>158</sup> United Nations, "Sustainability.", <https://www.un.org/en/academic-impact/sustainability>, Inter-Agency Space Debris Coordination Committee. (2025). *IADC Report on the Status of the Space Debris Environment* (Issue 3, IADC-23-01) p. 5

surveillance, and climate observation.<sup>159</sup> This has been affirmed by the UNGA in a resolution adopted on December 4th, 2024, stating that the UNGA is "*Deeply concerned* about the fragility of the space environment and the challenges to the long-term sustainability of outer space activities, in particular the impact of space debris, which is an issue of concern to all nations,"<sup>160</sup> Christopher J. Newman and Mark Williamson write that "space debris represents the primary threat" to the use of Outer Space.<sup>161</sup>

The Space environment is getting more and more congested, particularly in Low Earth Orbit (LEO), which hosts most active satellites.<sup>162</sup> It is in the LEO that we are seeing a drastic increase of launches, partly due to commercial actors entering the space-faring field.<sup>163</sup> The congestion is not limited to active satellites, but also inactive ones and a growing amount of debris. A large amount of data confirms the increase in space debris in the space environment. According to the European Space Agency, they estimate that as of May 5th, 2025, there have been an estimated 6910 launches of rockets since the beginning of the Space Age in 1957, and that these rockets have placed an estimated 21620 objects into the Earth's orbit.<sup>164</sup> The mass of all these space objects in Earth's orbit is over 14000 tons.<sup>165</sup> There is an estimated 120 million bits of debris.<sup>166</sup> The number of objects in Earth's orbit has increased substantially since the end of the Cold War, as indicated by data provided by The National Aeronautics and Space Administration, in the graph below.<sup>167</sup>

---

<sup>159</sup> Secure World Foundation, "Space Sustainability – A Practical Guide," 2018.

<sup>160</sup> United Nations General Assembly. (2024, December 12). *International cooperation in the peaceful uses of outer space* (A/RES/79/87). United Nations.

<sup>161</sup> Newman and Williamson, "Space Sustainability." p. 33

<sup>162</sup> Organisation for Economic Co-operation and Development, "Space Sustainability," (n.d.), <https://www.oecd.org/en/topics/space-sustainability.html>

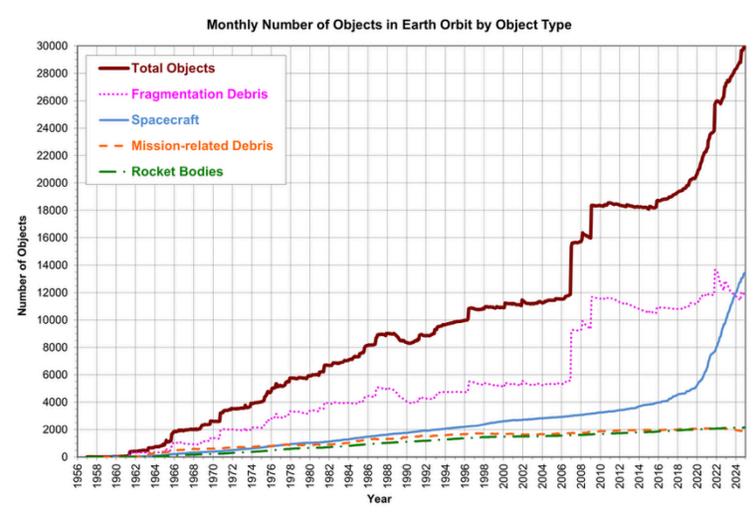
<sup>163</sup> Inter-Agency Space Debris Coordination Committee. (2025). *IADC Report on the Status of the Space Debris Environment* (Issue 3, IADC-23-01) p. 25

<sup>164</sup> European Space Agency, "Space Environment Statistics · Space Debris User Portal.", <https://sdup.esoc.esa.int/discosweb/statistics/>.

<sup>165</sup> Ibid.

<sup>166</sup> Bhattacharjee, N. (2024, December 2). *Global push for cooperation as space traffic crowds Earth orbit* <https://www.reuters.com/science/global-push-cooperation-space-traffic-crowds-earth-orbit-2024-12-02/>.

<sup>167</sup> National Aeronautics and Space Administration Orbital Debris Program Office. *Orbital Debris Quarterly News*, vol. 29, no. 1, Feb. 2025, <https://orbitaldebris.jsc.nasa.gov/quarterly-news/pdfs/ODQNv29i1.pdf>, p. 8



Source: The National Aeronautics and Space Administration

Statistically, according to the Organisation for Economic Co-operation and Development (OECD), as the number of objects in the Earth's orbit increases, there is an increased risk of accidental collisions, malfunction, and debris rises.<sup>168</sup> In their data, they argue that the likelihood of such a collision between a satellite and a "1 cm piece of debris" is about once every four years.<sup>169</sup>

Historically, these collisions have only occurred four times, per the European Space Agency.<sup>170</sup> In the next few decades, the Inter-Agency Space Debris Coordination Committee, estimates this will lead to a drastic increase in what they refer to as "catastrophic collisions."<sup>171</sup> This increases the likelihood of what is commonly, often referred to as the Kessler Syndrome.<sup>172</sup> Notably, interview data confirms this concern, with one participant further stating that "the space actor most concerned about space debris is the U.S. military," and what it identifies as a growing operational and security risk.<sup>173</sup>

<sup>168</sup> Organisation for Economic Co-operation and Development. *Earth's Orbits at Risk: The Economics of Space Sustainability*. OECD Publishing, 2022, p. 17

<sup>169</sup> Ibid.

<sup>170</sup> European Space Agency, "Space Environment Statistics · Space Debris User Portal.", <https://sdup.esoc.esa.int/discosweb/statistics/>.

<sup>171</sup> Inter-Agency Space Debris Coordination Committee. (2025). *IADC Report on the Status of the Space Debris Environment* (Issue 3, IADC-23-01) p. 25

<sup>172</sup> Andrew Ross Wilson and Massimiliano Vasile, "The Space Sustainability Paradox," p. 33

<sup>173</sup> Interview Data

Global governance in relation to this relies on voluntary norms and "best practice" guidelines. These are instruments of soft law that are helpful, but insufficient without political commitment and oversight, and that "soft law is all the same, if you do not commit to the major countries, it means nothing."<sup>174</sup> Examples of soft law, are the Debris Mitigation Guidelines that aims to mitigate the threat of overcrowding, such as the ones published by the United Nations Office for Outer Space Affairs, that outline recommendations, such as limiting debris that is created during space operations, minimize break-ups during its operational phase, limit the long-term presence of spacecraft and launch vehicles in the LEO, after they have completed their mission, limit the likelihood of accidental collisions and the avoidance of intentional destruction.<sup>175</sup> However, as was mentioned in one of our interviews, there is a lack of binding regulations and requirements in regards to active debris removal and collision avoidance. A concern over the absence of international enforcement mechanisms was echoed, and that again, this relies on an increase of transparency and trust among Space-faring States, as debris removal technology could serve a dual-purpose, hence it is "key to avoid suspicions from other countries."<sup>176</sup>

#### **(v) Ground-to-Ground Threats**

Ground-to-Ground threats are based on the ground and pose a threat to other objects on the ground, especially if they form part of a space system- like ground stations.<sup>177</sup> Ground-to-Ground threats include: a) Sabotage; b) Attacks on ground stations and terrorism; and c) Espionage. Ground stations can be defrauded from a physical, cyber, electromagnetic or internal standpoint. Any of these acts of fraud jeopardize the efficacy, integrity, and safety of space missions.<sup>178</sup>

---

<sup>174</sup> Interview Data

<sup>175</sup> United Nations General Assembly. *The "Space2030" Agenda: space as a driver of sustainable development*. Resolution A/RES/76/3, adopted on 25 October 2021.

<sup>176</sup> Interview Data

<sup>177</sup> Kaitlyn Johnson, "What Is Space Security and Why Does It Matter?" *Georgetown Journal of International Affairs* 20 (2019): p.83, <https://www.jstor.org/stable/26794945>.

<sup>178</sup> Consultative Committee for Space Data Systems (CCSDS), *The Application of Security to CCSDS Protocols: Informational Report CCSDS 350.0-G-3* (Washington, DC: CCSDS, 2019), 2-5.

## a) Sabotage

Sabotage can be defined as actions that cause damage, destruction, or compromise the regular functioning of a ground station<sup>179</sup>, usually carried out in a hidden or disguised manner. Cyber fraud includes unethical means of infiltrating systems, malware to corrupt data, ransomware, and spoofing those commands. Electromagnetic fraud may include jamming, spoofing of communications with satellites or polarization interference.<sup>180</sup>

Effective functioning of space systems relies on the supporting earthly infrastructure, or space segment, formed by the ground stations. These facilities enable satellites to perform communication, navigation, and remote sensing tasks by sending and receiving data.<sup>181</sup> They can be a potential target for sabotage. Ground station sabotage describes purposeful and hostile action to damage, disable, or disrupt the operation of a ground station. State or non-state actors, insiders, and cybercriminals can pursue these goals for reasons ranging from seeking political leverage to profiting from industrial or corporate espionage.<sup>182</sup>

Insider threats are still a major challenge, even in security settings. Employees and contractors with appropriate access credentials can be incentivized or persuaded to perform sabotage internally. Operations in ground stations are heavily dependent on human interaction and automated systems which introduce various methods through which sabotage can be accomplished.<sup>183</sup> Furthermore, the emergence of new space companies and small satellite missions have increased the number of commercial ground stations which widens the scope of risk.

---

<sup>179</sup> Justia. "Sabotage." *Justia Legal Dictionary*. Accessed May 15, 2025.

<https://dictionary.justia.com/sabotage>.

<sup>180</sup> Ibid.

<sup>181</sup> National Aeronautics and Space Administration (NASA), *Small Spacecraft Technology State of the Art: Ground Data Systems and Mission Operations* (Washington, DC: NASA, 2024),

<https://www.nasa.gov/wp-content/uploads/2025/02/soa-2024.pdf?emrc=d6f893>.

<sup>182</sup> Center for Strategic and International Studies (CSIS). "Space System Threats." *Aerospace Security*, September 2018. <https://aerospace.csis.org/wp-content/uploads/2018/09/Space-System-Threats.pdf>.

<sup>183</sup> NASA Office of Inspector General. *Audit of NASA's Insider Threat Program*. Washington, DC: NASA OIG, 2022. <https://oig.nasa.gov/docs/IG-22-009.pdf>.

## **b) Attacks on ground stations and terrorism**

Although satellites are guarded both spatially and with hostile surroundings, ground stations are situated within adverse physical territory open to intrusion and attack. An example of such an attack would be the terror attack against the Paris headquarters of the European Space Agency in 1984, with the building sustaining damage and six people being injured from flying glass as a result of a bomb.<sup>184</sup> Terrorist activity against space assets and facilities are also a ground-to-ground threat that, if employed, would affect space operations in any number of areas. Alternative forms could also include explosive or incendiary attacks (impacting power and control lines, antennas, and cables).

An attack on a ground station may result in disruptions to other sectors. The melding of military and civilian aims of some space systems amplifies both the absolute importance, and vulnerabilities of ground stations. Critical infrastructure systems, like national grids, air traffic control, and maritime navigation expand the threat surface. The interconnectivity means that attacking a ground station may have cascading effects to other sectors as well.<sup>185</sup>

In a world where States depend on one another to cooperate, shared ground station networks, and partnerships, striking one ground station will have affected multiple countries. Intra-State sabotage of critical infrastructure should not only be seen as a national security issue, but as an international concern.<sup>186</sup>

## **a) Espionage**

Internal fraud includes unethical practices that may be committed by undercover agents, such as employees or individuals with appropriate access credentials to the ground station and space

---

<sup>184</sup> Kozera, p.83.

<sup>185</sup> Palleti, Krishna, Osman Yağan, and H. Vincent Poor. “Cascading Effects of Cyber-Attacks on Interconnected Critical Infrastructure Systems.” *Cybersecurity* 4, no. 1 (2021): 1–14.  
<https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00071-z>.

<sup>186</sup> McCreight, Robert., “Gauging the Impact of Satellite & Space Systems on Critical Infrastructure,” *Journal of Homeland Security and Emergency Management* 20, no. 2 (2023): 198–199,  
<https://www.degruyterbrill.com/document/doi/10.1515/jhsem-2022-0054/html>.

systems can be incentivized or persuaded to perform sabotage or espionage activities (including foreign and corporate espionage).<sup>187</sup> The United States National Counterintelligence and Security Center released a bulletin informing both commercial stakeholders associated with the U.S. Space industry that foreign intelligence entities could approach their employees at conferences for recruitment, and that they may attempt to siphon intellectual property as well.<sup>188</sup>

Historical precedents provide evidence of possible risks concerning threats to ground stations. In 2008, NASA's Terra Earth observing satellite was hacked by persons unknown through a ground station on several occasions for a few minutes.<sup>189</sup> Although the hackers did not demonstrate altered operation nor issue commands, they showed a degree of capability to interfere at relatively advanced levels.<sup>190</sup> The same or similar gaps were found in the 2014 cyber attack on German Aerospace Center (DLR), where government hackers attempted to capture operational and storage systems and went as far as to attempt to capture the data.<sup>191</sup>

Legal mechanisms to deal with the issue, and protective and deterrent measures, are now absent despite the risk. The Outer Space Treaty and subsequent agreements cover space objects, actions, and orbits. In relation to the infrastructure on Earth it is normally the case that the national legal order will regulate it. There is no international law that generally regulates the attacks of ground stations. This lapse makes it difficult to coordinate, respond, and hold accountable at the international level.<sup>192</sup>

---

<sup>187</sup> National Counterintelligence and Security Center, "Safeguarding the US Space Industry: Keeping your Intellectual Property in Orbit," August 18th, 2023, p.1-2, <https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL%20FINAL%20Safeguarding%20the%20US%20Space%20Industry%20-%20Digital.pdf>.

<sup>188</sup> Ibid.

<sup>189</sup> Todd Harrison, Kaitlyn Johnson, and Thomas G. Roberts, "Space Threat Assessment 2018," Center for Strategic and International Studies (CSIS), April 2018, p.11, [https://aerospace.csis.org/wp-content/uploads/2018/04/Harrison\\_SpaceThreatAssessment\\_FULL\\_WEB.pdf](https://aerospace.csis.org/wp-content/uploads/2018/04/Harrison_SpaceThreatAssessment_FULL_WEB.pdf).

<sup>190</sup> Ibid.

<sup>191</sup> Security Affairs. Paganini, Pierluigi. "German Aerospace Center Hit By Serious Malware-Based Attack. April 16, 2014, <https://securityaffairs.com/24031/cyber-crime/german-aerospace-center-espionage.html>.

<sup>192</sup> Xu, Xiaojun, Qingyang Su, Vladimir Vernadskiy, Yadong Cheng, e Yun Zhou. "A Research on China–Russia Arms Control Cooperation in Outer Space." *Space: Science & Technology* 5, no. 1 (2024): 293–301. <https://link.springer.com/article/10.1007/s42533-024-00166-5>.

## (vi) Cyber Threats

The digitalization of space systems has increasingly linked space with cyberspace.<sup>193</sup> So much so that some satellites are now connected to the internet.<sup>194</sup> Coupled with the increasing prevalence of space systems in military and civilian uses, this expanding vulnerability drew quite a lot of attention. Although it is hard to provide exact numbers due to the nature of cyber attacks, their numbers have recently skyrocketed<sup>195</sup> leading more and more space security documents to emphasise cybersecurity. In general, cyberattacks are forms of interruptions to operational control and information flows of systems by the introduction of malware, denial of service attacks, downstream modification, etc.<sup>196</sup> However, cyber threats to space infrastructures give rise to very different dynamics than those to infrastructures on Earth, and than the other space threats.<sup>197</sup>

One aspect of this has to do with the nature of cyber attacks in general. The cybersecurity domain is usually asymmetric, providing the attacker with an advantageous position.<sup>198</sup> Due to the intangible and transboundary nature of cyberspace, while a kinetic attack can be observed from start-to-end, cyberattacks are hardly observable and even harder to attribute.<sup>199</sup> This plausible deniability is especially due to the “heterogeneous pool of threat actors”, ranging from nation-states to hacking groups.<sup>200</sup> For many States and non-state actors, acquiring the means for cyberattacks as a space security doctrine is much more realistic and affordable.<sup>201</sup> Cyber threats are also very hard to defend against because space systems have multiple connection and gateway points creating a variety of targets.<sup>202</sup> This means that a space system is vulnerable to

---

<sup>193</sup> Poirier, Clémence. Understanding cybersecurity in Outer Space, 2024.

<https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse343-EN.pdf>.

<sup>194</sup> Vessels, Ly, Kenneth Heffner, and Daniel Johnson. “Cybersecurity Risk Assessment for Space Systems.” *2019 IEEE Space Computing Conference (SCC)*, July 2019, 11–19. <https://doi.org/10.1109/spacecomp.2019.00006>.

<sup>195</sup> Poirier, 2.

<sup>196</sup> Hamill-Stewart, Jessie, and Awais Rashid. 2024. Threats Against Satellite Ground Infrastructure: A Retrospective Analysis of Sophisticated Attacks. Paper presented at the Workshop on Security of Space and Satellite Systems (SpaceSec), San Diego, CA, March 1.

<https://www.ndss-symposium.org/wp-content/uploads/spacesec2024-87-paper.pdf>.

<sup>197</sup> Ibid, 3.

<sup>198</sup> Yoon, Junghyun and Um, Jungsik. “Complex Challenges of Space Cybersecurity and Their Implications for the ROK.” *The Korean Journal of Defense Analysis* 36(3). 2024: 339-367. <https://doi.org/10.22883/kjda.2024.36.3.003>

<sup>199</sup> Poirier, 2.

<sup>200</sup> Ibid.

<sup>201</sup> Yoon and Um, 348-9.

<sup>202</sup> Ibid, 343.

cyber attacks in all three operational segments —ground, space and the link between the two— as well as throughout its operational cycle, from the supply chain to space operations.<sup>203</sup> Cyber attacks are also hard to pinpoint because an issue with a satellite has a similar likelihood of being caused by a malfunction as by a cyberattack, and cyberattacks can remain dormant for extended periods of time before being activated.<sup>204</sup> These factors put cyberattacks as a much cleaner and safer way to sabotage space activity of adversaries, especially incentivizing the actors with lesser space capabilities.<sup>205</sup>

Another aspect of space cybersecurity has to do with the nature of space and space operations. One limiting factor is that the lifespan of a space asset is long.<sup>206</sup> The cybersecurity protocols and encryption algorithms of these assets are bound to become outdated over the duration of its operation.<sup>207</sup> Conducting software updates to satellites are hazards themselves since they can interfere with unintended functions and create risks, which is what happened to Phobos 2 which lost its lock on the sun and depleted its energy. Because of their dependence on radio transmissions, updates also open a new gateway for an adversary to interfere with the satellite.<sup>208</sup> Additionally, the computing power aboard spacecrafts are necessarily limited, putting a strain on the length of cybersecurity protocols that can be implemented,<sup>209</sup> maintaining strong cybersecurity measures in space is a near-impossible task. On the other hand, once a satellite is deployed, the hardware of the satellite is inaccessible.<sup>210</sup> Hence, while a computer affected by a cyber attack can be unplugged, a satellite affected by a cyberattack cannot be interfered with apart from a cyber counterattack.<sup>211</sup> Additionally, the harsh space environment can corrupt digital information, including encryption keys, which require a flexible cybersecurity approach, posing another roadblock to defending against cyber attacks towards space systems.<sup>212</sup>

One last factor to consider in assessing cyber threats is the current situation of the space sector. Space is a commercialized sector where most of the military satellites too are used for both

---

<sup>203</sup> Varadharajan and Suri, 1.

<sup>204</sup> Yoon and Um, 340-349.

<sup>205</sup> *Ibid*, 344.

<sup>206</sup> Varadharajan and Suri, 4.

<sup>207</sup> Vessels et al, 12.

<sup>208</sup> *Ibid*, 11; Varadharajan and Suri, 4.

<sup>209</sup> Poirier, 3.

<sup>210</sup> Varadharajan and Suri, 3; CSS, 3.

<sup>211</sup> Poirier, 3.

<sup>212</sup> Varadharajan and Suri, 5.

private and military endeavors.<sup>213</sup> This commercial aspect leads to cybersecurity issues being insufficiently emphasized, mostly overlooked by a prioritization of latency and efficiency over security.<sup>214</sup> Not only that but the variety of actors and suppliers prevent the standardization, monitoring or integration of cybersecurity protocols and regulations.<sup>215</sup> The supply chain for space systems is dispersed among a large array of suppliers in different parts of the world. Component parts are sourced from various approved suppliers all around the world and assembled and operated by the space organization owning the space system, who consequently gets little say on the code and cybersecurity capabilities of the component parts.<sup>216</sup> This problem is exacerbated by the fact that usually the space assets and the infrastructure for the provision of the asset services are owned and operated by different organizations, creating more areas where cybersecurity cooperation is needed.<sup>217</sup>

Traditional cybersecurity standards are hence inadequate to respond to space cyber threats, which should be studied within the framework of these characteristics.<sup>218</sup> For these reasons, space cyber security is geared towards maintaining functional control of the space system given temporary losses of availability.<sup>219</sup> As a strategy, it is considered more viable and cost-effective to have the capability to attack an adversary's assets rather than defend yours from them, consequently more and more State and non-state actors are incentivized towards counter space cyber capabilities.<sup>220</sup> As a countermeasure, some States have engaged in cyber exercises regarding space assets and are formulating measures to retain operable capability in space in degraded conditions.<sup>221</sup>

Cyberattacks usually result in temporary and reversible effects on space systems. In fact, most cyberattacks that occur do not target the satellites but target the ground stations and networks.<sup>222</sup> Hence, the most common occurrence of cyberattacks are data stealing and service sabotage attacks. These include overloading systems, monitoring and tracking service recipients, stealing

---

<sup>213</sup> Yoon and Um, 344.

<sup>214</sup> Poirier, 3; Varadharajan and Suri, 1.

<sup>215</sup> Yoon and Um, 341.

<sup>216</sup> Varadharajan and Suri, 3.

<sup>217</sup> *Ibid*, 4.

<sup>218</sup> Poirier, 3.

<sup>219</sup> Vessels et al, 12.

<sup>220</sup> Yoon and Um, 341-2.

<sup>221</sup> Poirier, 3.

<sup>222</sup> *Ibid*, 2.

and corrupting sensitive data, etc.<sup>223</sup> Some attacks target the consumers as well, like interference with broadcasts and “spoofing” (providing false information to extract information).<sup>224</sup>

Since space systems operate in constellations and provide multiple services at once, these attacks can have spill-over effects. For example, a cyberattack towards a satellite on the eve of the invasion of Ukraine affected thousands of civilian customers outside Ukraine, including critical infrastructures.<sup>225</sup>

Cyberattacks can also target satellites themselves, which have more devastating effects. Some cyber attacks focus on satellite hijacking or denying control to the ground control center.<sup>226</sup> A simple denial-of-service attack on a satellite can make it lose the ability to maneuver, unable to avoid incoming objects or crashing into other satellites.<sup>227</sup> Not only locking the command centers out, cyber attacks can deliberately reroute satellites to destroy others.<sup>228</sup> While some of such attacks can be temporary and reversible, these attacks may result in the loss of the asset, shortening of its service lifespan or creation of space debris.<sup>229</sup>

Indicators show an increased exposure of satellites to cyber attacks.<sup>230</sup> Such attacks can be initiated at any stage of the satellite’s lifecycle: radio transmissions to it can be targeted, malware can be introduced in any part of the supply chain or by a personnel of the ground control center, etc.<sup>231</sup> Emerging technologies such as quantum computing and artificial intelligence make available new avenues for cybersecurity but also for cyber attacks.<sup>232</sup> A comprehensive policy solution needs to take into account the developments in space and cyberspace technology, which can only be done by the inclusion and cooperation of the various actors and stakeholders of the space sector.<sup>233</sup>

---

<sup>223</sup> Varadharajan and Suri, 2; Yoon and Um, 346.

<sup>224</sup> Poirier, 2.

<sup>225</sup> Ibid, 1.

<sup>226</sup> Varadharajan and Suri, 2; Yoon and Um, 346.

<sup>227</sup> Vessels et al, 11.

<sup>228</sup> Varadharajan and Suri, 2.

<sup>229</sup> Yoon and Um, 340.

<sup>230</sup> Vessels et al, 12.

<sup>231</sup> Ibid 11; Varadharajan and Suri, 2.

<sup>232</sup> Varadharajan and Suri, 5.

<sup>233</sup> Ibid, 7.

# Consequences for Space and Earth

## Consequences for Space

### Short Term Consequences

Short term consequences of space threats to space concern the disruption and degradation of operability and the increase of the risk of space operations.

Attacks and disruptions towards space assets end in temporary unavailability, destruction or shortening of operable lifespan of space systems. Attacks that cause temporary unavailability, such as dazzling and spoofing caused by electronic or cyber attacks, can cause risky situations since the disruption of data transfer may lead to avoidable collisions, loss of coordination in satellite constellations and disruption of the provision of services. Such temporary obstructions can also cause the lifespan of the assets to shorten<sup>234</sup>. Threats targeting space assets, such as space-to-space and ground-to-space threats, may end up in partial or complete destruction of the space asset, and in the loss of functionality in either case, rendering the spacecraft defunct.

One important short-term result of destructive force is the creation of space debris. When a satellite is destroyed, including via earth-based ASATs or co-orbital ASATs, it creates debris which remains in space, and which can harm space objects as well as future space activities.<sup>235</sup> Once in orbit, objects remain in orbit essentially indefinitely, accumulating and reaching tremendous speeds.<sup>236</sup> This creates a constant risk of collision with objects as little as a screw, which can render entire spacecraft inoperable upon impact. This increased risk also increases the cost of operating space assets.<sup>237</sup>

---

<sup>234</sup> Yoon and Um, 340

<sup>235</sup> Secure World Foundation, "Global Counterspace Capabilities," p. 42.

<sup>236</sup> Wright, Grego, and Gronlund, p. 22.

<sup>237</sup> Bongers and Torres, p. 828.

## Long Term Consequences

Some long term consequences of the denial, disruption, degradation, damage or destruction of space systems for outer space include: a build-up of debris; resource exploitation; an arms race and weaponization of space; militarization of space; and the blurring of civilian and military targets, making them indistinguishable.

If space debris increases over time (and remains there), there could be a Kessler syndrome effect where a growing cloud of debris may result in cascading collisions, rendering the orbit unusable.<sup>238</sup> ASAT tests in particular pose a grave risk to space security, but also to space systems, having created “nearly 5,000 pieces of orbital debris since the 1960s, more than 3,000 of which still pose navigation hazards to satellites.”<sup>239</sup> One expert said that this debris could make satellites economically unfeasible as they would have to contend with increased operational costs.<sup>240</sup> Another said that prolonged creation of debris would mean space as a global commons becomes “less efficient, less useful, less effective” and that this is a problem for everyone, including harm to a State’s own satellites.<sup>241</sup>

One of the interviewees stated that the idea of financially lucrative resources in space can cause a race for them, especially for commercial asteroid mining in the future.<sup>242</sup> They also likened this to the colonial competition for resources on Earth.<sup>243</sup> If commercial interests in Space are not matched with proper controls on the management of resources in space, this could contribute to the exploitation of resources and international tension.<sup>244</sup> Furthermore, resource exploitation can create new risks, such as meteoroids and the alteration of asteroid trajectories (which could in

---

<sup>238</sup> Cyprian Aleksander Kozera and Pawel Bernat, “Space Terrorism: A Historical Study,” *Safety and Defense* 9 (2). March 6th, 2024, p.81, <https://doi.org/10.37105/sd.217>.

<sup>239</sup> Victoria Samson and Brian Weeden, “Enhancing Space Security: Time for Legally Binding Measures,” *Arms Control Today* 50, no. 10 (2020): p.10, <https://www.jstor.org/stable/26975486>.

<sup>240</sup> Interview Data.

<sup>241</sup> Ibid.

<sup>242</sup> Interview Data.

<sup>243</sup> Ibid.

<sup>244</sup> Henry Padden, “Does Space Law Prevent Patterns of Antarctic Imperialism in Outer Space?” *Global Policy* 13, April 2022, p.355, <https://doi.org/10.1111/1758-5899.13104>.

turn impact Earth).<sup>245</sup> Another long-term consequence of Ground-to-Space threats is the risk of an intensified arms race in space, contributing to increased weaponization of space. An intensified arms race would mean higher costs, increased weapons testing (decreasing the safe use of space), and potential escalation into a full-scale war.<sup>246</sup>

## Consequences for Earth

### Short Term Consequences

The threats assessed in this research have consequences on Earth that have immediate effects on our everyday life, as much of our critical infrastructure relies on space-based technologies, such as banking and financial systems. Something as simple as using an ATM would not be possible if Space systems were to be damaged. Airports would be unable to use air traffic control, and ships at sea would be without a navigational system. In the United Kingdom, if there were a loss of Global Navigation Satellite Systems (GNSS) for a seven-day period, the economic loss is estimated to be around 7.2 billion British Pounds.<sup>247</sup>

For example, if satellite service disruption were to occur, the impact would be immediate with continued reverberating effects, GPS systems would not work, affecting not only civilian life, but military operations, significantly reducing the “operational capacity”, as weapons such as drones and guided bombs rely on GPS.<sup>248</sup> Additionally, the lack of meteorological data would significantly affect civilian life as it aids in natural disaster prevention, occurrences that are becoming more and more common due to climate change and the lack of data in relation to agriculture would affect food production.<sup>249</sup> The agricultural impact would affect food

---

<sup>245</sup> Michael Byers and Aaron Boley, “Chapter 5: Space Mining” in *Who Owns Outer Space?: International Law, Astrophysics, and the Sustainable Development of Space*, Cambridge Studies in International and Comparative Law, Cambridge: Cambridge University Press, 2023, p. 136-137, <https://www.cambridge.org/core/books/who-owns-outer-space/960CCB0464744F845B09434D932699EC>.

<sup>246</sup> Mutschler, p.10.

<sup>247</sup> London Economics *The Economic Impact on the UK of a Disruption to GNSS* Issue 4: 2021 Update, Final Report, August 2023, p. 2

<sup>248</sup> Bongers and Torres, p. 827.

<sup>249</sup> World Meteorological Organization. “Early Warnings for All,” February 15, 2024. <https://earlywarningsforall.org/site/early-warnings-all>.

production. Healthcare systems relying on telemedicine would be affected, and medical supply chains would be unworkable. Something as simple as calling an ambulance would simply not be possible.<sup>250</sup>

There would be immediate consequences to the loss of communication with satellites. These disruptions can include the suspension of communications and loss of data transmissions. As a plethora of industries rely on an uninterrupted satellite information flow, any disruption poses serious safety and operational concerns. Additionally, through cyberattacks there is a risk that that sensitive information could be breached or lost during system disruptions.<sup>251</sup>

Economic consequences occur when commercial satellite service providers suffer contractual penalties for service interruptions within the agreed periods, resulting in lost business, diminished reputation, and breach of trust. In addition, local communities suffer complex power and local infrastructure damage.<sup>252</sup>

According to the Global Risk Report 2022, produced by the World Economic Forum, we do not yet know the impacts that increasing space use has had on the Earth's environment, such as the ozone layer.<sup>253</sup> Additionally, they argue that the increasing tension and the subsequent space race have demanded higher government spending on space programs, especially from the dominant space-faring actors, while for the majority of the Earth's governments, these technologies will remain inaccessible.<sup>254</sup> As mentioned, the impact of these consequences would be disproportionately felt across the world. Developing nations are more vulnerable to some of these consequences. They might have less backup systems and fewer alternatives to use if their primary system were to fail.

---

<sup>250</sup> United Nations Office for Outer Space Affairs, "Benefits of Space: Global Health.", <https://www.unoosa.org/oosa/de/benefits-of-space/global-health.html>.

<sup>251</sup> John T. Correll, "Destiny in Space," Air & Space Forces Magazine, August 1, 1998, <https://www.airandspaceforces.com/article/0898edit/>.

<sup>252</sup> European Union Agency for Cybersecurity (ENISA), Space Threat Landscape 2025, March 26, 2025, <https://www.enisa.europa.eu/publications/enisa-space-threat-landscape-2025>.

<sup>253</sup> World Economic Forum *The Global Risks Report 2022* (17th ed.) World Economic Forum, 2022 [https://www3.weforum.org/docs/WEF\\_The\\_Global\\_Risks\\_Report\\_2022.pdf](https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf), p. 76

<sup>254</sup> Ibid.

## Long Term Consequences

This section will examine the long term consequences that could be provoked by deliberate threats against space systems and ground stations and how they would affect global cooperation and the future sustainability of space activities on Earth.

There is a risk of escalation to an armed conflict on Earth, particularly through attacks on space-based assets and ground stations. Multiple interviewees noted that an armed attack would have to be deliberate, and that the law of armed conflict (as well as international law) would still apply regarding space systems.<sup>255</sup> However, if there was a deliberate attack on a space system asset or on a ground station, this could increase the risk of an escalation to an armed conflict. One expert noted that in the event of an armed conflict, space system components can be legitimate targets.<sup>256</sup> As a long-term consequence, this could cause confusion between the civilian and military space infrastructure, increasing the risks to space security. The empowerment of hostile States, terrorist factions, or criminal groups to carry out attacks against stations may also represent a long-term consequence of space-related threats to Earth.<sup>257</sup>

Nations could nationalize their terrestrial infrastructure, which could reduce international collaboration and capital inflows into the space infrastructure sector. This could divide the international space community and undermine coordinated action to advance sustainable practices in outer space.<sup>258</sup> Also, commercial actors will encounter regulatory uncertainty that will create riskier operations, and will, in turn, actively discourage investment.<sup>259</sup>

Another long-term consequence could be the transformation of the legal and political paradigm.

---

<sup>255</sup> Interview Data.

<sup>256</sup> Ibid.

<sup>257</sup> Hamill-Stewart, Jessie, and Awais Rashid. 2024. Threats Against Satellite Ground Infrastructure: A Retrospective Analysis of Sophisticated Attacks. Paper presented at the Workshop on Security of Space and Satellite Systems (SpaceSec), San Diego, CA, March 1. <https://www.ndss-symposium.org/wp-content/uploads/spacesec2024-87-paper.pdf>.

<sup>258</sup> United Nations. "Outer Space Becoming Contested Domain for Supremacy with Space-Based Communications, Intelligence Assets, Anti-Satellite Weapons, First Committee Hears." United Nations Meetings Coverage and Press Releases, October 19, 2023. <https://press.un.org/en/2023/gadis3722.doc.htm>.

<sup>259</sup> McCreight, Robert, "Gauging the Impact of Satellite & Space Systems on Critical Infrastructure," Journal of Homeland Security and Emergency Management 20, no. 2 (2023): 198–199, <https://www.degruyterbrill.com/document/doi/10.1515/jhsem-2022-0054/html>.

States could be motivated to submit proposals for new international agreements or expand existing ones to eliminate references to terrestrial infrastructure. Disagreements over definition, application, enforcement and attribution are plausible obstacles to progress. Over time, the gaps in interpretation of the space legal system may erode the coherence of the international legal regime governing outer space.<sup>260</sup>

One tangible symptom of political fractures is the decline in joint space initiatives and the slow unraveling of longstanding partnerships. The once-robust collaboration between The National Aeronautics and Space Administration (NASA) and Roscosmos (Russian Space Agency), a hallmark of post-Cold War space diplomacy, has weakened significantly in recent years.<sup>261</sup> Ongoing geopolitical tensions, such as the Russian invasion of Ukraine have further strained any bilateral and multilateral space activities. In an interview, an example of the future of the International Space Station (ISS) was given. Continuing what was once a symbol of peaceful cooperation, now appears uncertain as national priorities diverge, and funding commitments are reconsidered. Interviewees noted that national space programs are often tied to domestic political agendas, making them vulnerable to cuts, populist skepticism, or policy turnover.<sup>262</sup>

This fragmentation contributes to the erosion of global governance structures. The relationship between State and private actors is becoming increasingly blurred, as major private launch companies (such as SpaceX, Blue Origin) provide critical services to multiple nations.<sup>263</sup> As aforementioned, one expert noted that States do not necessarily need their own launch systems to be spacefaring.<sup>264</sup> This disrupts traditional power hierarchies and forces the reevaluation of what it means to be a “space actor.” Interview participants also pointed out that “most countries are spacefaring in the sense that they have satellites or purchase satellite services,” but lack launch infrastructure. This structural dependence leaves them vulnerable to the risks generated by dominant actors.

---

<sup>260</sup> Dionysia-Theodora Avgerinopoulou, “Current Trends and Challenges in International Space Law,” in 53rd Meeting of the European Space Sciences Committee, Athens, Greece, May 2017, [https://www.essc.esf.org/wp-content/uploads/2021/09/53rd\\_Athens17\\_Avgerinopoulou\\_Article\\_Current\\_Trends\\_and\\_Challenges\\_in\\_Space\\_Law.pdf](https://www.essc.esf.org/wp-content/uploads/2021/09/53rd_Athens17_Avgerinopoulou_Article_Current_Trends_and_Challenges_in_Space_Law.pdf).

<sup>261</sup> Grunert, “The Future of Western-Russian Civil-Space Cooperation.”

<sup>262</sup> Interview Data.

<sup>263</sup> Weinzierl, Matthew and Mehak, Sarang. “The Commercial Space Age Is Here,” *Harvard Business Review*, February 12, 2021. <https://hbr.org/2021/02/the-commercial-space-age-is-here>

<sup>264</sup> Interview Data.

Also, a long-term consequence of threats to space infrastructure includes reduced access to satellite-based climate data collections. Satellites are very important for monitoring environmental changes and global climate measurements. The scientific community can be greatly harmed by the lack of accurate data. Its absence impacts the ability of governments to implement actions and weakens the systems that are needed to address climate change.

Threats posed to the space environment can also exacerbate global inequality. Many developing countries have become increasingly reliant on satellites operated by foreign entities to provide services in communication, navigation, emergency services and disaster response, and development planning. Interruptions in accessing satellite services (from conflict, commercialization, or degradation of infrastructure) could deepen existing gaps between nations. Long-term, this could create development stalls in vulnerable geographic areas and sustain geopolitical unbalances that undermine global efforts for equitable and sustainable development.

---

## Conclusion

As this report has discussed, space is an integral and indispensable part of life as it provides many essential services, ranging from communications and navigation to climate monitoring and disaster response. Throughout this research, we have aimed to map the landscape of threats that pose a risk to these systems and the consequences that would follow their disruption, degradation, or destruction.

There has been an identification and categorization of various threats to space security, including political threats driven by geopolitical competition, ground-to-space threats like direct-ascent ASATs, space-to-ground threats such as kinetic bombardment, space-to-space threats including co-orbital ASATs, ground-to-ground threats targeting infrastructure, and cyber and electronic threats that exploit digital vulnerabilities. However, it is important to note that these threats, while categorized separately in this report, are interconnected.

There should also be acknowledgement that the perspectives of the Global South are often overlooked in discussions of space security. While there has been some democratization of space access, the dialogue remains dominated by major space powers.

The consequences of these threats are manifested both in space and on earth, with both short and long-term implications. In the short term, consequences include, for example, the destruction of space assets, creation of orbital debris, immediate disruptions to Earth-based services dependent on space systems, economic losses, and reduced military capabilities. Long-term, we face risks such as orbits rendered unusable, potential escalation to armed conflict, increasing nationalism in space policy at the expense of international cooperation, reduced access to shared climate data, blurring lines between civilian and military space assets, and further exacerbation of global inequalities.

Space-based systems are increasingly becoming vulnerable both in orbit and on earth. As we continue to grow more dependent on space, the mitigating of these threats through various measures, such as improving international cooperation, further developing norms for responsible behavior, and inclusive governance frameworks, are some of the ways we can preserve a world where space and access to it remain for generations to come.

## Bibliography

- Abeyratne, Dr. Ruwantissa I.R. "Cyber Terrorism and Activities in Outer Space." *Tolley's Communications Law* 5 no. 1, 2000. p.419.  
[https://www.elevenjournals.com/tijdschrift/iisl/1999/4%20Other%20Issues%20of%20Space%20Law/IISL\\_1999\\_042\\_004\\_018.pdf](https://www.elevenjournals.com/tijdschrift/iisl/1999/4%20Other%20Issues%20of%20Space%20Law/IISL_1999_042_004_018.pdf).
- African Union, "Agenda 2063: The Africa We Want." Addis Ababa: African Union Commission, 2015.
- Alshdaifat, Shadi A. and Silverburg, Sanford R. "Can Terrorism Mold Itself to Outer Space? An International Legal Perspective." *International Journal of Cyber Warfare and Terrorism* 11 no. 2 (April 2021): p.56.  
[https://www.researchgate.net/publication/350561942\\_Can\\_Terrorism\\_Mold\\_Itself\\_to\\_Outer\\_Space\\_An\\_International\\_Legal\\_Perspective](https://www.researchgate.net/publication/350561942_Can_Terrorism_Mold_Itself_to_Outer_Space_An_International_Legal_Perspective).
- Arnould, Jacques. "Ethics of Planetary Science and Exploration." *Oxford Research Encyclopedia of Planetary Science* (2020) <https://doi.org/10.1093/acrefore/9780190647926.013.234>.
- Azcárate Ortega, Almudena and Victoria Samson (Eds.). "A Lexicon for Outer Space Security." UNIDIR. Geneva. August 16th, 2023.  
[https://unidir.org/wp-content/uploads/2023/09/UNIDIR\\_Lexicon\\_for\\_Outer\\_Space\\_Security.pdf](https://unidir.org/wp-content/uploads/2023/09/UNIDIR_Lexicon_for_Outer_Space_Security.pdf).
- Bhattacharjee, Nivedita, and Nivedita Bhattacharjee. "Global Push for Cooperation as Space Traffic Crowds Earth Orbit." *Reuters*, December 2, 2024, sec. Science. Accessed on April 28th,  
<https://www.reuters.com/science/global-push-cooperation-space-traffic-crowds-earth-orbit-2024-12-02/>.
- Blatt, Talia. "ANTI-SATELLITE WEAPONS AND THE EMERGING SPACE ARMS RACE." *Harvard International Review* 41, no. 3 (2020). Gale Academic OneFile, p.30.  
<https://link.gale.com/apps/doc/A699459154/AONE?u=hei&sid=bookmark-AONE&xid=0db5af02>.
- Bongers, Anelí and José L. Torres. "Star Wars: Anti-Satellite Weapons and Orbital Debris." *Defence and Peace Economics* 35, no. 7 (2023): p.830. <https://doi.org/10.1080/10242694.2023.2208020>.
- Botti, F., & Greco, E. (Eds.). (2023). *The Geopolitics of Space*.
- Center for Development of Security Excellence (CDSE), "Risk Management for DoD Security Programs Training Glossary". Accessed on April 29th,  
<https://www.cdse.edu/Portals/124/Documents/glossary/GS102-glossary.pdf>.
- Center for Strategic and International Studies (CSIS). "Space System Threats." Aerospace Security, September 2018. Accessed on April 29th 2025.  
<https://aerospace.csis.org/wp-content/uploads/2018/09/Space-System-Threats.pdf>.
- Center for Strategic and International Studies (CSIS), "Space Threat Assessment 2021". Accessed on April 29th.  
[https://aerospace.csis.org/wp-content/uploads/2021/03/CSIS\\_Harrison\\_SpaceThreatAssessment2021.pdf](https://aerospace.csis.org/wp-content/uploads/2021/03/CSIS_Harrison_SpaceThreatAssessment2021.pdf).
- Cesari Laetitia. "What's in a Word? Notions of 'Security' and 'Safety' in the Space Context → UNIDIR." UNIDIR, May 12, 2023.  
<https://unidir.org/whats-in-a-word-notions-of-security-and-safety-in-the-space-context/>.

Byers, Michael, and Aaron Boley. *Who Owns Outer Space?: International Law, Astrophysics, and the Sustainable Development of Space*. Cambridge Studies in International and Comparative Law. Cambridge: Cambridge University Press, 2023.

<https://www.cambridge.org/core/books/who-owns-outer-space/960CCB0464744F845B09434D932699EC>

Cerny, Michael B., Raphael J. Piliero, David Bernstein, and Brandon W. Kelley, “Countering Co-Orbital ASATs: Warning Zones in GEO as a Lawful Trigger for Self- Defense,” Study Report, May 2020.

Chagos Marine Protected Area Arbitration *Mauritius v. United Kingdom*, (2011). Accessed November 20, 2024. <https://pca-cpa.org/en/cases/11/>.

Chandrashekar, S. “India and the Peaceful Uses of Outer Space.” *India Review* 10, no. 4 (October 1, 2011): 440–52. <https://doi.org/10.1080/14736489.2011.624034>.

Cheng, Bin. *Studies in International Space Law*. Oxford: Clarendon, 1997.

Chow, Brian G. “Stalkers in Space: Defeating the Threat.” *Strategic Studies Quarterly* 11, no. 2 (2017): 82–116. <http://www.jstor.org/stable/26271574>.

Consultative Committee for Space Data Systems (CCSDS), *The Application of Security to CCSDS Protocols: Informational Report CCSDS 350.0-G-3* (Washington, DC: CCSDS, 2019), 2-5.

Correll. “Destiny in Space.” *Air & Space Forces Magazine* (blog). Accessed May 16, 2025.

<https://www.airandspaceforces.com/article/0898edit/>.

Cottam, Jamie. “How to Prevent a War in Space (Part 1).” The Cove (Australian Army). November 7th, 2022. <https://cove.army.gov.au/article/how-prevent-war-space-part-1>.

Cottam, Jamie. “How to Prevent a War in Space (Part 2).” The Cove (Australian Army). November 8th, 2022. <https://cove.army.gov.au/article/how-prevent-war-space-part-2>.

Davis, Rian, Bace Brianna, and Unal Tatar. “Space as a Critical Infrastructure: An in-Depth Analysis of U.S. and EU Approaches.” *Acta Astronautica* 225 (December 2024): 263–72.

<https://doi.org/10.1016/j.actaastro.2024.08.053>.

Dawson, Linda. *The Politics and Perils of Space Exploration: Who Will Compete, Who Will Dominate?* Springer Nature, pp. 2-11 (2021).

Delegation of Brazil. “Destructive Anti-satellite Weapons.” Open-ended working group on reducing space threats through norms, rules and principles of responsible behaviours. A/AC.294/2023/WP.13. February 6th, 2023. United Nations General Assembly.

[https://documents.un.org/symbol-explorer?s=A/AC.294/2022/WP.16&i=A/AC.294/2022/WP.16\\_3739988](https://documents.un.org/symbol-explorer?s=A/AC.294/2022/WP.16&i=A/AC.294/2022/WP.16_3739988)

Dennerley, Joel A. “State Liability for Space Object Collisions: The Proper Interpretation of ‘Fault’ for the Purposes of International Space Law.” *European Journal of International Law* 29, no. 1 (May 8, 2018): 281–301. <https://doi.org/10.1093/ejil/chy003>.

Dionysia-Theodora Avgerinopoulou, “Current Trends and Challenges in International Space Law,” in 53rd Meeting of the European Space Sciences Committee, Athens, Greece, May 2017. Accessed on April 29th 2025.

[https://www.essc.esf.org/wp-content/uploads/2021/09/53rd\\_Athens17\\_Avgerinopoulou\\_Article\\_Current\\_Trends\\_and\\_Challenges\\_in\\_Space\\_Law.pdf](https://www.essc.esf.org/wp-content/uploads/2021/09/53rd_Athens17_Avgerinopoulou_Article_Current_Trends_and_Challenges_in_Space_Law.pdf).

Drake, Nadia. “Where, Exactly, Is the Edge of Space? It Depends on Who You Ask.” National Geographic. December 20, 2018. Accessed on 18/11/2024.

<https://www.nationalgeographic.com/science/article/where-is-the-edge-of-space-and-what-is-the-karman-line>.

Fraes, Gabriel Elefteriu. “The Role of Space Power in Geopolitical Competition.” *Council of Geostrategy - Geopolitics Programme*, no. No. GPPR01 (January 2024).

<https://www.geostrategy.org.uk/app/uploads/2024/02/The-role-of-space-power-in-geopolitical-competitionGPPR01.pdf>.

European Parliament. “EU space strategy for security and defence.” (2023) Accessed on April 29th 2025

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754598/EPRS\\_BRI%282023%29754598\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/754598/EPRS_BRI%282023%29754598_EN.pdf).

European Space Policy Institute. “The Rise of Private Actors in the Space Sector: Executive Summary.” (2017).

European Space Agency, “Space Environment Statistics · Space Debris User Portal.” Accessed May 16, 2025. <https://sdup.esoc.esa.int/discosweb/statistics/>.

European Union Agency for Cybersecurity (ENISA), Space Threat Landscape 2025, March 26, 2025, accessed May 2025 <https://www.enisa.europa.eu/publications/enisa-space-threat-landscape-2025>.

Fetter, Steve. “Protecting our Military Space Systems” in Edmund S. Muskie, ed. *The U.S. in Space: Issues and Policy Choices for a New Era* (Washington DC: Center for National Policy Press 1988). 1-25.

<https://cisssm.umd.edu/sites/default/files/2019-08/1988-CNP-ASAT.pdf>.

Francis, Lyall and Paul B. Larsen. *Space Law: A Treatise*, Ashgate Publishing, 2010, Accessed November 20, 2024. [https://law.adelaide.edu.au/ua/media/861/ALR\\_39%282%29\\_08\\_Lisk.pdf](https://law.adelaide.edu.au/ua/media/861/ALR_39%282%29_08_Lisk.pdf).

Gil, H.E. Laura. “Statement of the G-77 and China during the sixty-seventh session of the United Nations Committee on the Peaceful Uses of Outer Space,” 19-28 June 2024,

[https://www.unoosa.org/documents/pdf/copuos/2024/statements/5\\_G77andChina.pdf](https://www.unoosa.org/documents/pdf/copuos/2024/statements/5_G77andChina.pdf).

Garrido Guijarro, Gabriel. “A Common African Outer Space Policy to Meet the Continent’s Challenges.” Instituto Español de Estudios Estratégicos. November 16, 2022. Accessed May 3rd, 2025

[https://www.ieee.es/Galerias/fichero/docs\\_analisis/2022/DIEEEA73\\_2022\\_OSCGAR\\_Espacio\\_ENG.pdf](https://www.ieee.es/Galerias/fichero/docs_analisis/2022/DIEEEA73_2022_OSCGAR_Espacio_ENG.pdf).

Grego, Laura. “A History of Anti-Satellite Programs.” Union of Concerned Scientists. January 2012.

[https://www.ucs.org/sites/default/files/2019-09/a-history-of-ASAT-programs\\_lo-res.pdf](https://www.ucs.org/sites/default/files/2019-09/a-history-of-ASAT-programs_lo-res.pdf).

Grego, Laura. “Security in Space: What Is at Stake and How Do We Move Forward?” *Asian Perspective* 35, no. 4 (2011): p.511 <http://www.jstor.org/stable/42704769>.

Grunert, J. (2022, May 26). *The Future of Western-Russian Civil-Space Cooperation*. War on the Rocks. <https://warontherocks.com/2022/05/the-future-of-western-russian-civil-space-cooperation/>.

Gurevich, Vladimir. “New Strategy is Needed to Solve the 50-Year-Old Problem - EMP Protection of Critical Civilian Infrastructure.” *International Journal of Emerging Science and Engineering* 12, no. 2: January 2024. <https://www.ijese.org/wp-content/uploads/Papers/v12i2/L255711111223.pdf>.

Guterres, António. “Reducing space threats through norms, rules and principles of responsible behaviours: Report of the Secretary-General” July 13th, 2021. United Nations General Assembly. 76th session. [https://documents.un.org/symbol-explorer?s=A/76/77&i=A/76/77\\_3095022](https://documents.un.org/symbol-explorer?s=A/76/77&i=A/76/77_3095022).

Hamill-Stewart, Jessie, and Awais Rashid. 2024. Threats Against Satellite Ground Infrastructure: A Retrospective Analysis of Sophisticated Attacks. Paper presented at the Workshop on Security of Space and Satellite Systems (SpaceSec), San Diego, CA, March 1. Accessed on April 29th 2025 <https://www.ndss-symposium.org/wp-content/uploads/spacesec2024-87-paper.pdf>.

Harrison, Todd. “Framework for Evaluating Space Weapons.” *International Perspectives on Space Weapons*. Center for Strategic and International Studies (CSIS), 2020. <http://www.jstor.org/stable/resrep24829.6>.

Harrison, Todd, Kaitlyn Johnson, and Thomas G. Roberts. “Space Threat Assessment 2018.” Center for Strategic and International Studies (CSIS). April 2018. [https://aerospace.csis.org/wp-content/uploads/2018/04/Harrison\\_SpaceThreatAssessment\\_FULL\\_WEB.pdf](https://aerospace.csis.org/wp-content/uploads/2018/04/Harrison_SpaceThreatAssessment_FULL_WEB.pdf).

Harrison, Todd, Zack Cooper, Kaitlyn Johnson, and Thomas G. Roberts. “THREATS TO SPACE SYSTEMS.” *ESCALATION AND DETERRENCE: IN THE SECOND SPACE AGE*. Center for Strategic and International Studies (CSIS). 2017. <http://www.jstor.org/stable/resrep23194.4>.

Iderawumi, Mustapha. “Space Debris Delays Flights to South Africa Amid Warnings of Falling Rocket Components.” *Space in Africa*. January 25th, 2025. <https://spaceinafrica.com/2025/01/25/space-debris-delays-flights-to-south-africa-amid-warnings-of-falling-rocket-components/>.

Inter-Agency Space Debris Coordination Committee. (2025). *IADC Report on the Status of the Space Debris Environment* (Issue 3, IADC-23-01)

Institut Montaigne, *The Geopolitics of a New Modern Space Race*. (n.d.). Retrieved April 14, 2025, from <https://www.institutmontaigne.org/en/expressions/geopolitics-new-modern-space-race>.

Jaramillo, Cesar. “The Multifaceted Nature of Space Security Challenges.” *Space Policy* 33 (August 2015): 63–66, <https://doi.org/10.1016/j.spacepol.2015.02.007>.

Johnson, Kaitlyn. “What Is Space Security and Why Does It Matter?” *Georgetown Journal of International Affairs* 20 (2019): 81–85. <https://www.jstor.org/stable/26794945>.

Johnson, Kaitlyn. “Rendezvous and Proximity Operations.” *Key Governance Issues in Space*. Center for Strategic and International Studies (CSIS), 2020. <http://www.jstor.org/stable/resrep26047.7>.

Justia. “Sabotage.” *Justia Legal Dictionary*. Accessed May 15, 2025. <https://dictionary.justia.com/sabotage>.

Klinger, Julie Michelle. "Critical Geopolitics of Outer Space." *Geopolitics* 26, no. 3 (May 3, 2021): 661–65. <https://doi.org/10.1080/14650045.2020.1803285>.

Kozera, Cyprian Aleksander and Pawel Bernat. "Space Terrorism: A Historical Study." *Safety and Defense* 9 (2). March 6th, 2024. <https://doi.org/10.37105/sd.217>.

Krishnan, Vineeth and Anupama Vijayakumar. "Assessing Continuities and Changes in Japan's Space Security Blueprint 2023." *Strategic Analysis* 47, no. 5 (September 3, 2023): 465–77. <https://doi.org/10.1080/09700161.2023.2288992>.

Kurian, Rosemary and Karamala Areesh Kumar. "The Emerging Threat Landscape of Space Terrorism." *Modern Diplomacy*. May 9th 2024. Accessed on November 9th, 2024. <https://modern diplomacy.eu/2024/05/09/the-emerging-threat-landscape-of-space-terrorism/>.

Lee, Ricky J. "LIABILITY ARISING FROM ARTICLE VI OF THE OUTER SPACE TREATY: STATES, DOMESTIC LAW AND PRIVATE OPERATORS." *International Institute of Space Law*, no. 3 (2005): 216–28.

Lele, Ajay. "Space Terrorism: Is it a Possibility?" March 7th, 2003. Institute of Peace and Conflict Studies, [https://www.ipcs.org/comm\\_select.php?articleNo=981](https://www.ipcs.org/comm_select.php?articleNo=981).

Lisk, Joel. "Space Law: A Treatise." *Adelaide Law Review*, 2018 Accessed November 20, 2024, [https://law.adelaide.edu.au/ua/media/861/ALR\\_39%282%29\\_08\\_Lisk.pdf](https://law.adelaide.edu.au/ua/media/861/ALR_39%282%29_08_Lisk.pdf).

London Economics *The Economic Impact on the UK of a Disruption to GNSS* Issue 4: 2021 Update, Final Report, August 2023,

Mabuni, Brandt, and Mark Bryan Manantan. "Accelerating Asia-Pacific Space Economies Through Regional Partnerships." *Indo-Pacific Affairs* 1, no. 1 (November 1, 2024): 1–3.

Macron, Emmanuel. "Prononcé Le 11 Décembre 2023 - Emmanuel Macron 11122023 Plan France 2030 | Vie-Publique.Fr." Déclaration de M. Emmanuel Macron, président de la République, sur la politique économique du gouvernement, à Toulouse le 11 décembre 2023, November 12, 2023. Accessed May 12 2025, <https://www.vie-publique.fr/discours/292373-emmanuel-macron-11122023-plan-france-2030>.

Markram, Thomas. "Possible Challenges to Space Security and Sustainability," *Arms Control Today* 47, no. 10 (2017): p.44, <https://www.jstor.org/stable/90016032>.

McCreight, Robert., "Gauging the Impact of Satellite & Space Systems on Critical Infrastructure," *Journal of Homeland Security and Emergency Management* 20, no. 2 (2023): 198–199, Accessed on April 29th 2025. <https://www.degruyterbrill.com/document/doi/10.1515/jhsem-2022-0054/html>.

Meyer, Paul. "The United Nations Security Council Takes up Space Security – It Might Have Been Best If It Had Not." *Open Canada* (blog), June 17, 2024. <https://opencanada.org/the-united-nations-security-council-takes-up-space-security-it-might-have-been-best-if-it-had-not/>.

Miller, Gregory D. "Space Pirates, Geosynchronous Guerrillas, and Nonterrestrial Terrorists," *Air and Space Power Journal*. (Fall 2019), p.39, [https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-33\\_Issue-3/F-Miller.pdf](https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-33_Issue-3/F-Miller.pdf).

Ming, Zhang. “The Space Silk Road and China–Arab States Space Cooperation.” *INSIGHTS*, no. No. 309 (November 6, 2024). Pp. 3-15

Mutschler, Max M. “The Danger of an Arms Race in Space.” *Keeping Space Safe: Towards a Long-Term Strategy to Arms Control in Space*. Peace Research Institute Frankfurt, January 1st, 2010.  
<http://www.jstor.org/stable/resrep14496.4>.

National Aeronautics and Space Administration, Orbital Debris Program Office. *Orbital Debris Quarterly News*, vol. 29, no. 1, Feb. 2025,  
<https://orbitaldebris.jsc.nasa.gov/quarterly-news/pdfs/ODQNv29i1.pdf>.

National Aeronautics and Space Administration (NASA), Small Spacecraft Technology State of the Art: Ground Data Systems and Mission Operations (Washington, DC: NASA, 2024). Accessed on April 29th 2025  
<https://www.nasa.gov/wp-content/uploads/2025/02/soa-2024.pdf?emrc=d6f893>.

NASA. The Artemis Accords (2020). Accessed November 21, 2024,  
<https://www.nasa.gov/wp-content/uploads/2022/11/Artemis-Accords-signed-13Oct2020.pdf?emrc=673fa5bdcdb1d>.

National Counterintelligence and Security Center. “Safeguarding the US Space Industry: Keeping your Intellectual Property in Orbit.” August 18th, 2023.  
<https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL%20FINAL%20Safeguarding%20the%20US%20Space%20Industry%20-%20Digital.pdf>.

New Space Economy. “Understanding the Ethical Landscape of the Space Economy.” Understanding the Ethical Landscape of the Space Economy, August 27, 2023. Accessed October 20th, 2024,  
<https://newspaceeconomy.ca/2023/08/27/understanding-the-ethical-landscape-of-the-space-economy/>.

Newman, Christopher J., and Mark Williamson. “Space Sustainability: Reframing the Debate.” *Space Policy* 46 (November 2018): 30–37. <https://doi.org/10.1016/j.spacepol.2018.03.001>.

Ngcofe, Luncedo. “Is There Enough Space for Africa in Outer Space?” *South African Journal of Science* 121, no. 3–4 (April 2025): 1–4. <https://doi.org/10.17159/sajs.2025/18777>.

Ochmanek, David and Lowell H. Schwartz. “The Uniquely Destructive Capabilities of Nuclear Weapons.” In *The Challenge of Nuclear-Armed Regional Adversaries*, 1st ed., 5–14. RAND Corporation, 2008. <http://www.jstor.org/stable/10.7249/mg671af.10>.

Oduntan, Gbenga. *Sovereignty and Jurisdiction in the Airspace and Outer Space: Legal Criteria for Spatial Delimitation*, Routledge Research in International Law. London: Routledge, (2019)

Organisation for Economic Co-operation and Development. “Space Sustainability.” OECD. (n.d). Accessed November 14th, 2024, <https://www.oecd.org/en/topics/space-sustainability.html>.

OECD (2022), *Earth’s Orbits at Risk: The Economics of Space Sustainability*, OECD Publishing, Paris, <https://doi.org/10.1787/16543990-en>.

Padden, Henry. “Does Space Law Prevent Patterns of Antarctic Imperialism in Outer Space?” *Global Policy* 13, (2022): 346–357. <https://doi.org/10.1111/1758-5899.13104>.

Palleti, Krishna, Osman Yağan, and H. Vincent Poor. “Cascading Effects of Cyber-Attacks on Interconnected Critical Infrastructure Systems.” *Cybersecurity* 4, no. 1 (2021): 1–14. Accessed on April 29th 2025. <https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00071-z>.

Peperkamp, Lonneke. “An Arms Race in Outer Space?” *Atlantisch Perspectief* 44, no. 4 (2020): 46–50. <https://www.jstor.org/stable/10.2307/48600572>.

Petr Boháček, Topic 3: Current and Future Space-to-Space Threats by States to Space Systems, Agenda Item 6(b), Open-Ended Working Group on Reducing Space Threats Through Norms, Rules and Principles of Responsible Behaviours, Second session, Geneva (14 Sep. 2022).

Plotnek, Jordan and Jill Slay. “New Dawn for Space Security.” *International Conference on Cyber Warfare and Security* 17, no. 1 (March 2, 2022): 253–61. <https://doi.org/10.34190/iccws.17.1.17>.

Pobjie, Erin and Almudena Azcárate Ortega. “Space Security Legal Primer 1- Outer Space & Use of Force,” UNIDIR, September 2024, p.11. [https://unidir.org/wp-content/uploads/2024/09/UNIDIR\\_Outer\\_Space\\_and\\_Use\\_of\\_Force.pdf](https://unidir.org/wp-content/uploads/2024/09/UNIDIR_Outer_Space_and_Use_of_Force.pdf).

Poirier, Clémence. Understanding cybersecurity in Outer Space, 2024. [https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalys\\_e343-EN.pdf](https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalys_e343-EN.pdf).

Porras, Daniel. “Anti-Satellite Warfare and the Case for an Alternative Draft Treaty for Space Security,” *Bulletin of the Atomic Scientists* 75, no. 4 (2019): p.142 <https://doi.org/10.1080/00963402.2019.1628470>.

Putin, Vladimir. “Meeting on Development of Space Activities.” President of Russia, April 20, 2025. Accessed on May 12 2025, <http://en.kremlin.ru/events/president/news/76692>.

Pynnöniemi, K., & Jokela, M. (2020). Perceptions of hybrid war in Russia: means, targets and objectives identified in the Russian debate. *Cambridge Review of International Affairs*, 33(6), 828–845. Accessed on April 29th. <https://www.tandfonline.com/doi/full/10.1080/09557571.2020.1787949>.

Quinland, Roger. “Galactic Governance: From the Outer Space Treaty to Modern Regulations.” (2024). Accessed November 21 2024, <https://www.thespacereview.com/article/4843/1>.

Rajagopalan, Rajeswari Pillai. “Space Security in the Indo-Pacific.” *Air and Space Law* 48, no. Special Issue (March 1, 2023): 59–74 <https://doi.org/10.54648/AILA2023031>.

Rajagopalan, Rajeswari Pillai. “Space and Cyber Global Governance: A View from the Global South.” Centre for International Governance Innovation. January 29th, 2023. Accessed November 26, 2024. <https://www.cigionline.org/articles/space-and-cyber-global-governance-a-view-from-the-global-south/>.

Rathgeber, Wolfgang, and Remuss, Nina-Louisa. “Space Security. A Formative Role and Principled Identity for Europe.” European Space Policy Institute, January 16, 2009. <https://www.espi.or.at/reports/space-security-a-formative-role-and-principled-identity-for-europe/>.

Samson, Victoria and Brian Weeden. “Enhancing Space Security: Time for Legally Binding Measures,” *Arms Control Today* 50, no. 10 (2020): p.6, <https://www.jstor.org/stable/26975486>.

- Samson, Victoria. (2021, August 12). *The Geopolitics of a New Modern Space Race*. Institut Montaigne. Accessed, February 23, 2025. <https://www.institutmontaigne.org/en/expressions/geopolitics-new-modern-space-race>.
- Samson, Victoria. "Fact sheet: U.S. Co-Orbital Anti-Satellite Testing." Secure World Foundation. December 2024. [https://swfound.org/media/207999/fs24-07\\_us-co-orbital-anti-satellite-testing.pdf](https://swfound.org/media/207999/fs24-07_us-co-orbital-anti-satellite-testing.pdf).
- Samson, Victoria and Laetitia Cesari. "Global Counterspace Capabilities Report 2025." Secure World Foundation. April 3rd, 2025. [https://swfound.org/media/208099/swf\\_global\\_counterspace\\_capabilities\\_2025.pdf](https://swfound.org/media/208099/swf_global_counterspace_capabilities_2025.pdf).
- Secure World Foundation. "Space Sustainability – A Practical Guide," 2018.
- Sheehan, Michael. "Viewpoint: Space Security and Developing Nations." *Space Policy* 37 (August 2016): 20–23. <https://doi.org/10.1016/j.spacepol.2016.10.005>.
- Spies, Michael. "A Human-Centered Approach to Outer Space Security: How to Boost UN Efforts in the near-Term." Humanitarian Law & Policy Blog. November 9, 2023. <https://blogs.icrc.org/law-and-policy/2023/11/09/human-centered-approach-to-outer-space-security-how-to-boost-un-efforts/>.
- Space Training and Readiness Command (STARCOM). *Space Doctrine Publication 3-0, Operations*. United States Space Force, 2023.
- Space Sustainability—Astroscale, Securing Space Sustainability. (n.d.). *Astroscale*. Retrieved April 15, 2025, from <https://astroscale.com/space-sustainability/>.
- Steer, Cassandra. "Global Commons, Cosmic Commons: Implications of Military and Security Uses of Outer Space." *Georgetown Journal of International Affairs* 18, no. 1 (2017): p.9. <http://www.jstor.org/stable/26396047>.
- Stefanovich, Dmitry, and Daniel Porras. "Space as a Competition Domain: Threats and Opportunities." *Journal of International Analytics* 13, no. 2 (2022), p.101. [https://www.researchgate.net/profile/Dmitry-Stefanovich/publication/361603643\\_Space\\_as\\_a\\_Competition\\_Domain\\_Threats\\_and\\_Opportunities/links/62bdab1e88d96f1e6b2f9ae8/Space-as-a-Competition-Domain-Threats-and-Opportunities.pdf](https://www.researchgate.net/profile/Dmitry-Stefanovich/publication/361603643_Space_as_a_Competition_Domain_Threats_and_Opportunities/links/62bdab1e88d96f1e6b2f9ae8/Space-as-a-Competition-Domain-Threats-and-Opportunities.pdf).
- Shmigol, Valerie. "The United States Is Enabling an Outer Space Arms Race: An Overview of the Current Framework and Recommendations for Abating an Outer Space Arms Race." *Seattle University Law Review* 46, no. 1 (2022): 175–200. Accessed on April 29th <https://digitalcommons.law.seattleu.edu/sulr/vol46/iss1/7/>.
- Stroikos, Dimitrios. "Still Lost in Space? Understanding China and India's Anti-Satellite Tests through an Eclectic Approach," *Astropolitics* 21 vol.2–3 (2023): p.179. <https://doi.org/10.1080/14777622.2023.2277253>.
- Synder, Randall J. "Space Law: Past, Present, and Future. By Carl Q. Christol. Deventer/Boston: Kluwer Law and Taxation Publishers, 1991. Pp. Xv, 516. Dfl. 195.00; US \$59.00 (Paper Bound)." *International Journal of Legal Information* 20, no. 2 (1992): 201–2. <https://doi.org/10.1017/S0731126500007861>.

The Ministry of Foreign Affairs of the Russian Federation. The Foreign Policy Concept of the Russian Federation. March 31, 2023. Accessed on April 29th, 2025.

[https://mid.ru/en/foreign\\_policy/fundamental\\_documents/1860586/](https://mid.ru/en/foreign_policy/fundamental_documents/1860586/).

The Ministry of Foreign Affairs of the Russian Federation. Statement by the Representative of the Delegation of the Russian Federation at the Thematic Discussion on “Outer Space (Disarmament Aspects)” in the First Committee of the 79th session of the UN General Assembly, New York, October 29, 2024. Accessed on April 29th.

[https://mid.ru/en/foreign\\_policy/news/1978174/?TSPD\\_101\\_R0=08765fb817ab2000e5de439d1c79638a2203927a352bc12e32f12659d1c00b35a1f57d65880c8b9d080f95f249143000d1d2f7561529d8bdc8ab85835fb1e6ede76b476022d0054bc4c597018f0ef0c8dcc6794ffe113d380049da3dd065d3f5](https://mid.ru/en/foreign_policy/news/1978174/?TSPD_101_R0=08765fb817ab2000e5de439d1c79638a2203927a352bc12e32f12659d1c00b35a1f57d65880c8b9d080f95f249143000d1d2f7561529d8bdc8ab85835fb1e6ede76b476022d0054bc4c597018f0ef0c8dcc6794ffe113d380049da3dd065d3f5).

The State Council Information Office of the People’s Republic of China. “China’s National Defense in the New Era.” Center for Strategic and International Studies. Accessed on April 29th 2025.

<https://www.csis.org/analysis/chinas-new-2019-defense-white-paper>.

The State Council. The Peoples Republic of China. “China's Space Program: A 2021 Perspective.” Accessed on April 29th 2025.

[https://english.www.gov.cn/archive/whitepaper/202201/28/content\\_WS61f35b3dc6d09c94e48a467a.html](https://english.www.gov.cn/archive/whitepaper/202201/28/content_WS61f35b3dc6d09c94e48a467a.html).

The Union of Soviet Socialist Republics, the United Kingdom of Great Britain and Northern Ireland and the United States of America. “Treaty banning nuclear weapon tests in the atmosphere, in outer space and under water.” 15th October, 1963.

<https://treaties.un.org/doc/Publication/UNTS/Volume%20480/volume-480-I-6964-English.pdf>.

Toyoma, Gentoku. “Countering Threats in Space Through International Cooperation,” Kidlington: Elsevier Ltd. – *Space policy* 55, (2021-02), Article 101387. DOI: [10.1016/j.spacepol.2020.101387](https://doi.org/10.1016/j.spacepol.2020.101387).

UN Office for Outer Space Affairs. “*Liability Convention* (1972).” Accessed November 19, 2024.

<https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introliability-convention.html>.

UN Office for Outer Space Affairs. “*Outer Space Treaty* (1967).” Accessed November 19, 2024.

<https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html>.

UN Office for Outer Space Affairs. “*Registration Convention* (1976).” Accessed November 20, 2024.

<https://www.unoosa.org/oosa/sk/ourwork/spacelaw/treaties/introregistration-convention.html>.

United Nations General Assembly. “Prevention of an arms race in outer space.” A/RES/75/35. December 7th, 2020. 75th Session. <https://digitallibrary.un.org/record/3895439?ln=en&v=pdf>.

United Nations General Assembly. “Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies.” December 19th, 1966. Resolution 2222 (XXI). [https://www.unoosa.org/pdf/gares/ARES\\_21\\_2222E.pdf](https://www.unoosa.org/pdf/gares/ARES_21_2222E.pdf).

United Nations General Assembly. (2024, December 12). *International cooperation in the peaceful uses of outer space* (A/RES/79/87). United Nations.

United Nations Office for Outer Space Affairs, “Benefits of Space: Global Health.” Accessed May 16, 2025. <https://www.unoosa.org/oosa/de/benefits-of-space/global-health.html>.

United Nations. “Outer Space Becoming Contested Domain for Supremacy with Space-Based Communications,

Intelligence Assets, Anti-Satellite Weapons, First Committee Hears.” United Nations Meetings Coverage and Press Releases, October 19, 2023. <https://press.un.org/en/2023/gadis3722.doc.htm>.

United Nations. “Sustainability.” United Nations. United Nations. Accessed May 14, 2025. <https://www.un.org/en/academic-impact/sustainability>.

United Nations General Assembly. *The “Space2030” Agenda: space as a driver of sustainable development*. Resolution A/RES/76/3, adopted on 25 October 2021. [https://www.unoosa.org/res/oosadoc/data/resolutions/2021/general\\_assembly\\_76th\\_session/ares763\\_html/A\\_RES\\_76\\_3\\_E.pdf](https://www.unoosa.org/res/oosadoc/data/resolutions/2021/general_assembly_76th_session/ares763_html/A_RES_76_3_E.pdf).

United Nations. “*Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space* (1963).” Accessed November 20, 2024. [https://www.unoosa.org/pdf/gares/ARES\\_18\\_1962E.pdf](https://www.unoosa.org/pdf/gares/ARES_18_1962E.pdf).

United Nations Institute for Disarmament Research. “Space Security - Terminology - Outer Space Security Lexicon,” n.d, accessed on May 2nd 2025. <https://spacesecuritylexicon.org/terminology/space-security>.

UNIDIR. “Threats to the security of space activities and systems.” Open-ended working group on reducing space threats through norms, rules and principles of responsible behaviours. A/AC.294/2022/WP.16. September 12th, 2022. United Nations General Assembly. [https://documents.un.org/symbol-explorer?s=A/AC.294/2022/WP.16&i=A/AC.294/2022/WP.16\\_3739988](https://documents.un.org/symbol-explorer?s=A/AC.294/2022/WP.16&i=A/AC.294/2022/WP.16_3739988)

United Nations Office for Outer Space Affairs. (2022). *Guidelines for the Long-term Sustainability of Outer Space Activities of the Committee on the Peaceful Uses of Outer Space*. United Nations. <https://doi.org/10.18356/9789210021852>.

United Nations, “*Threats to the security of space activities and systems*,” Submitted by the United Nations Institute for Disarmament Research (UNIDIR). Accessed on April 29th. [https://documents.unoda.org/wp-content/uploads/2022/08/20220817\\_A\\_AC294\\_2022\\_WP16\\_E\\_UNIDIR.pdf](https://documents.unoda.org/wp-content/uploads/2022/08/20220817_A_AC294_2022_WP16_E_UNIDIR.pdf)

United States Space Force. “Space Doctrine Publication (SDP) 3-0, Operations.” (2023).

United States Space Force. “THE CASE FOR CHANGE: Optimizing for Great Power Competition.” (n.d).

United States. U.S. Code Title 50 – War and National Defense, Section 3003: Definitions. Accessed April 11, 2025. <https://uscode.house.gov/view.xhtml?edition=prelim&num=0&req=granuleid%3AUSC-prelim-title50-section3003>.

Varadharajan, Vijay, and Neeraj Suri. *Security challenges when space merges with Cyberspace*, 2023. <https://doi.org/10.2139/ssrn.4474611>.

Vessels, Ly, Kenneth Heffner, and Daniel Johnson. “Cybersecurity Risk Assessment for Space Systems.” *2019 IEEE Space Computing Conference (SCC)*, July 2019, 11–19. <https://doi.org/10.1109/spacecomp.2019.00006>.

Vittitoe, Charles N. “Did High-Altitude EMP Cause the Hawaiian Streetlight Incident?” Sandia National Laboratories. June 1989. <https://ece-research.unm.edu/summa/notes/SDAN/0031.pdf>.

Weinzierl, Matthew and Mehak, Sarang. “The Commercial Space Age Is Here.” *Harvard Business Review*, February 12, 2021. <https://hbr.org/2021/02/the-commercial-space-age-is-here>.

White House. Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems. September 4, 2020. Accessed on April 29th <https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/>.

Wilson, Andrew Ross and Vasile, Massimiliano. “The Space Sustainability Paradox.” *Journal of Cleaner Production* 423 (October 15, 2023): 138869. <https://doi.org/10.1016/j.jclepro.2023.138869>.

World Economic Forum *The Global Risks Report 2022* (17th ed.) World Economic Forum, 2022 , accessed on May 4 2025 [https://www3.weforum.org/docs/WEF\\_The\\_Global\\_Risks\\_Report\\_2022.pdf](https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf).,

World Meteorological Organization. “Early Warnings for All,” February 15, 2024. Accessed on May 16, 2025 <https://earlywarningsforall.org/site/early-warnings-all>.

Wright, David, Laura Grego, and Lisbeth Gronlund. “The Physics of Space Security: A Reference Manual.” American Academy of Arts & Sciences. 2005. <https://aerospace.csis.org/wp-content/uploads/2019/06/physics-space-security.pdf>.

Wu, Xiaodan. “China and Space Security: How to Bridge the Gap between Its Stated and Perceived Intentions.” *Space Policy* 33 (August 2015): 20–28. <https://doi.org/10.1016/j.spacepol.2015.05.002>.

Yan, Yongliang. “Capacity Building in Regional Space Cooperation: Asia-Pacific Space Cooperation Organization.” *Advances in Space Research* 67, no. 1 (January 2021): 597–616. <https://doi.org/10.1016/j.asr.2020.10.022>.

Yoon, Junghyun and Um, Jungsik. “Complex Challenges of Space Cybersecurity and Their Implications for the ROK.” *The Korean Journal of Defense Analysis* 36(3). 2024: 339-367. <https://doi.org/10.22883/kjda.2024.36.3.003>.

Zahoor, Saadia. “Maintaining International Peace and Security by Regulating Military Use of Outer Space.” *Policy Perspectives* 14, no. 2 (2017): p.122. <https://doi.org/10.13169/polipers.14.2.0113>.

Zhou, Wen. “War, Law and Outer Space: Pathways to Reduce the Human Cost of Military Space Operations.” *Humanitarian Law & Policy*, 2023. <https://blogs.icrc.org/law-and-policy/2023/08/15/war-law-outer-space-reduce-human-cost-of-military-space-operations/>.

## Annex

Tentative Interview Questions, sent to all interviewees prior to the interview and forming the basis of the semi-structured interview:

### 1. Self-Introduction

- Could you describe your academic background in the field of space and space threats?
- Could you describe your role and professional expertise in the field of space and space threats?

### 2. Identification of Space Threats

- In your opinion, are there different perspectives and definitions for what constitutes a space threat? If yes, how does this impact mitigating space threats?
- In your opinion, what are the most pressing threats concerning space today?

### 3. What is Vulnerable in Space

- Are there particular vulnerabilities you think need urgent attention?
- What can you say about the dual-purpose nature of space technologies? Is there a concept of “strictly limited to civilian use” when it comes to space objects?

### 4. International Collaboration and Multilateralism

- What are your thoughts on the role of international collaboration in mitigating space threats? To what extent can multilateralism overcome space threats?
- How can States balance competition and cooperation in space?
- “The military uses of space inevitably cause some opacity and competition.” Do you agree with this statement?

### 5. Actors in Space

- Are States with no presence in space adequately included in dialogue on space threats? If not, how could this be facilitated?

- In your opinion, is it likely that non-State actors, including terrorist groups, would be able to use and target space systems in the future?

6. Solutions/Suggestions Regarding Space Threats

- Are there any current policies or frameworks you think are ineffective or in need of revision?

7. Future trends and interviewees

- Where would you recommend we look for data on future trends related to space threats?
- Would you have any recommendations for future interviewees we might contact to incorporate diverse perspectives on space threats?
- Are there any final comments or additional insight that you would like to share?