Acta Astronautica 234 (2025) 73–86

Contents lists available at ScienceDirect

Acta Astronautica

journal homepage: www.elsevier.com/locate/actaastro

The protection of AI-based space systems from a data-driven governance perspective

Giovanni Tricco [a,*], Roser Almenar [b,**], Kaili Ayers [c], Rihab Ben Moussa [d], Thomas Graham [e], Simisola Iyiola [f], Sanghoon Lee [g], Terezie Němcová [h], Asiimwe Joshua Opota [i], Tushar Sharma [j], Raelee Toh [k], Jieyu Yuan [l]

[a] Alma Mater Studiorum - University of Bologna, Italy
[b] University of Valencia, Spain
[c] Space Generation Advisory Council (SGAC), United States
[d] Space Generation Advisory Council (SGAC), Tunisia
[e] Swinburne University of Technology, Australia
[f] Space Generation Advisory Council (SGAC), United Kingdom
[g] Korea National Diplomatic Academy, Republic of Korea
[h] Friedrich-Alexander-Universität Erlangen-Nürnberg, Czech Republic
[i] Space Generation Advisory Council (SGAC), Uganda
[j] OP Jindal Global University, India
[k] Space Generation Advisory Council (SGAC), Republic of Singapore
[l] Space Generation Advisory Council (SGAC), the Netherlands

ARTICLE INFO

Keywords:
Artificial intelligence
Space law
Intellectual property
Cybersecurity
Data sharing
Dual-use systems

ABSTRACT

Space infrastructures have long represented the pinnacle of technological and engineering achievements. This complexity has been further amplified by the advent of the new space race, where private actors are taking the lead, alongside states, in deploying thousands of satellites in outer space. The outer space environment of 2040 will look very different from today. Spacecraft will necessitate more frequent maneuvers to avoid potential collisions, with the need to be more conscious of their surroundings. Indeed, as the frequency of events and the number of space objects rises, decision-making tasks will increasingly challenge human operators, especially as physical and temporal margins diminish. Such complexity is enveloping thanks to the synergy of space technologies and Artificial Intelligence (AI), which is transforming the functioning of space systems.

The forward trajectory clarifies the significance that AI in outer space will retain in the years ahead. The *Corpus Juris Spatialis* finds itself at a crossroads, faced with the defiance of withstanding the technological advances catalyzed by the impending integration of AI into all facets of space missions. Given the ubiquitous nature of AI, its implementation will invariably pose multifaceted legal challenges across diverse aspects of International Space Law. The acquired autonomy of space assets prompts crucial questions regarding the legal standards applicable to AI in outer space, and how these autonomous space systems should be protected against hostile interference.

The main purpose of this paper, presented by the Space Law and Policy Project Group of the Space Generation Advisory Council (SGAC), is to examine the pivotal legal dimensions stemming from the automation of space-based applications from a 'data-driven governance' standpoint. The increase in production and acquisition of space data will just augment the sophistication of AI systems, therefore necessitating their data assets to be reliable, accurate, and consistent to safeguard the long-term success of AI technologies in space missions. The paper aims to address the overarching legal challenges posed by the integration of AI into outer space operations,

This article is part of a special issue entitled: 2024 75th IAC Milan published in Acta Astronautica.

* Corresponding author.
** Corresponding author.
E-mail addresses: giovanni.tricco2@unibo.it (G. Tricco), roser.almenar@uv.es (R. Almenar), kaili.ayers@gmail.com (K. Ayers), benmousarihab@gmail.com (R. Ben Moussa), thomasgraham@swin.edu.au (T. Graham), simiiyiola@gmail.com (S. Iyiola), william931201@outlook.com (S. Lee), terezienemcova@gmail.com (T. Němcová), asiimweopota@gmail.com (A.J. Opota), tsharma2@jgu.edu.in (T. Sharma), raelee.toh.2021@law.smu.edu.sg (R. Toh), JenneyYuanNL@gmail.com (J. Yuan).

https://doi.org/10.1016/j.actaastro.2025.04.063
Received 10 January 2025; Received in revised form 13 March 2025; Accepted 30 April 2025
Available online 2 May 2025

specifically on cybersecurity, intellectual property, and data governance, which are critical for safeguarding autonomous systems. By examining the various nuances of these domains, it seeks to contribute to a comprehensive understanding of the legal landscape of the current AI-space pairing. Ultimately, the conclusion will offer a set of recommendations to pave the way for a secure, ethical evolution of autonomous space systems in the near future.

1. Introduction

The space industry is experiencing a significant transformation, driven by a combination of factors including a reduction in launch costs, the advent of fully reusable launch vehicles, a growing number of space-based applications, and the imminent deployment of numerous mega-constellations. These developments are expected to drive a considerable increase in the number of objects operating in the Low Earth Orbit (LEO) and beyond in the coming decades [1].

Given the intrinsic characteristics of the outer space environment and the pervasive digitalization within this field, it is evident that the implementation of Artificial Intelligence (AI) represents a compelling necessity. The space sector is witnessing a growing reliance on machine intelligence and assistance in a multitude of operational domains, including the launch, operation, maintenance, control, coordination, repair, and ultimate success of advanced commercial or military missions.

Indeed, the European Space Agency (ESA) foresees that "Artificial Intelligence is becoming vital to handle this complexity, to operate, network, coordinate and protect our space infrastructure and to get the most out of the data acquired by our scientific satellite missions" [2]. Mission success is therefore contingent upon the deployment of sophisticated computer-assisted models and algorithms, as well as robotics and communication systems that facilitate operations over vast distances in outer space [3]. The integration of data-driven methodologies into space activities is steadily gaining traction as a common approach.

The forward trajectory serves to illustrate the enduring significance of AI in the space domain in the years ahead. The field of space law is at a crossroads, confronted with the challenge of maintaining its relevance in the face of rapid technological advancement. The impending integration of new technologies, such as AI, into all aspects of space missions has the potential to substantially alter the current legal landscape. In light of the pervasive presence of AI, its integration will inevitably give rise to a multitude of interwoven regulatory issues. The discipline of space law will become increasingly intertwined with other legal domains, including data governance, cybersecurity, dual-use, and intellectual property.

Although we find this line of research still in its infancy, it is unquestionably important to foster the debate and increase the awareness of the space community about the possible new legal and policy challenges that we may end up experiencing in the not-too-distant future. To this effect, this paper deals with and attempts to answer these upcoming challenges by analyzing the case for the involvement of AI in space activities and navigating the different legal and policy concerns that the international community is irremediably destined to face.

Indeed, space law faces different challenges with the increasing digitalization of space activities. While liability issues in AI-driven missions have attracted some attention, different equally important questions remain largely unexplored.

This paper focuses on four particularly important, data-centric challenges at the intersection of AI and space activities: data sharing, cybersecurity, dual-use implications, and intellectual property rights (IP).

Questions around data sharing revolves around whether current regulations adequately sustain the international sharing of data while safeguarding personal information. Cybersecurity considerations, tackle the risk that AI poses for satellite networks and other essential infrastructure, especially as adversarial attacks and software vulnerabilities become more sophisticated. AI's dual-use nature further complicates the blurred line between civilian and military space activities, raising new policy and legal dilemmas under existing legal framework. Finally, IP issues multiply as AI systems generate vast quantities of novel data, testing the limits of current frameworks for ownership and authorship.

With the analysis of these selected four key domains, the paper aims to present a comprehensive, but focused analysis. These challenges have been insufficiently examined in ongoing discourse, and it is important to address them to shape a regulatory landscape that can keep pace with technological innovation. This research will be a foundation for further study and collaboration on how AI will reshape both space law and the governance of space activities.

2. Applications of AI in space activities

AI refers to "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments". This definition corresponds to those provided by both the Organisation for Economic Cooperation and Development (OECD) [4] and the European Union's AI Act [5].

AI comprises both Machine Learning (ML) and Deep Learning (DL) [6]. On the one hand, machine learning allows computers to learn without being programmed to do so, and can be found in tools such as chatbots and predictive text [7]. This means that algorithms can discern patterns and predict outcomes based on the training data. On the other hand, deep learning is a form of machine learning that is especially suitable for processing large amounts of data with reduced human intervention. Similar to how neurons in the human brain function, deep learning relies on neural networks to process data [8].

AI has already seen its application in the space context. According to ESA, AI is being used to control mega-constellations and to process and evaluate the data collected by such satellites [9]. Indeed, AI has the potential to improve the way satellite operators manufacture satellites, and therefore use data generated from their space objects. For instance, in the manufacturing phase, AI technologies can be utilized to perform repetitive tasks without human intervention, such as cleaning and updating the health status of components [2]. When these satellites are eventually launched into space, AI technologies can be instrumental in gathering more accurate space data while, at the same time, reducing costs [10].

Given these immense benefits, national and supranational space agencies like ESA, the French space agency CNES (*Centre national d'études spatiales*), and the US National Aeronautics and Space Administration (NASA) have invested in and funded projects to determine whether AI can be better applied to improve data collection [11,12]. Private entities have also leveraged AI technologies to improve processes. By way of example, SpaceX uses an AI autopilot system for its Falcon 9 craft to carry out docking with the International Space Station (ISS), and AI algorithms to ensure that its satellites do not collide with other space objects [13].

2.1. Needs, benefits, and challenges: what the future holds

As alluded to, AI has been used in traditional space applications, including remote sensing and monitoring, communications between

ground operators and the space segment, and data analytics [14]. Moreover, it sustains unmanned operations including satellite manufacturing and potentially in-orbit assembling of space infrastructures in the future. This has been done in the context of NASA personnel in the International Space Station (ISS), who have prototyped a set of AI algorithms to improve the capacities of the ISS [15]. Additionally, NASA employs the AI system "AEGIS" to build three-dimensional terrain maps aimed at finding out rock features and soil composition to recommend the day's activities based on factors like terrain complexity, energy usage, and scientific value [16].

Future use of AI could expand to deep space missions from the Moon to Mars, as well as to other celestial bodies, and potentially to asteroid mining and exploitation of space resources. For instance, China's University of Science and Technology invented an AI-powered robot that uses extracts from Mars to create oxygen from water, representing AI's potential to be used for chemical discovery [17]. The European Space Operations Centre (specifically, the MEXAR2) is also utilizing AI technologies in its endeavor, concretely, by making use of AI to resolve data downloading problems, which is now a vital part of the Mars exploration system [18].

Overall, the use of AI heralds manifold benefits for humankind in outer space, which can be summarized into the following: firstly, AI analyzes data more efficiently by identifying patterns, anomalies, and correlations that might otherwise go unnoticed; secondly, AI tools can optimize mission routes and schedules, decrease costs, and maximize scientific findings; and thirdly, AI is also already being employed to discern patterns in historical space weather data [19].

However, the growing integration of AI in space systems is also met with major obstacles, which can be classified into two main categories: those of a practical nature, and those about regulations. To begin with, the practical challenges associated with the application of AI technologies into the space sector concern the training of algorithms, especially deep learning models, which require significant computational resources, making it cumbersome to develop on resource-constrained shared devices. Moreover, the advancement of AI needs to be in tandem with potential cybersecurity threats, which pose a serious risk in the outer space context [20].

As for legal hindrances, the question arises as to whether AI can coexist with the current international space law regime, specifically under the 1967 Outer Space Treaty (OST) [21] and the 1972 Liability Convention (LIAB) [22], as will be discussed throughout the paper. In light of the use of AI, questions arise as to the meaning of "fault": should AI be used to substitute human decisions? Is the State of the software developer who was in charge of training the algorithm the one at fault [23] or should the AI system have its own legal personality? What does "fault" mean in legal terms? However, these questions will not be profoundly dealt with, as it does not suit the main purpose of the present paper.

2.2. The importance of software-base systems: AI on the edge

The use of software to support space missions has been on the increase over the years [24]. As shown before, the space industry, space agencies, and governments rely on the use of AI for their space plans and missions. In recent times, the industry has experienced an increase in the use of AI –particularly, in machine learning– to facilitate core functions such as launch, operation, maintenance, and repair of spacecraft and objects [3]. For example, ESA has implemented the use of AI in detecting signs of past or present life on Mars [20]. In the case of NASA, both the Remote Agent Experiment (RAX) in 1999 and the Autonomous Sciencecraft Experiment deployed in 2003 validated appropriate uses of AI-based capabilities in space activities [25]. Daily operations of missions, including the ISS, utilize different software for activities like crew and life support, autonomous systems, and environmental science [26, 27].

According to Piyush, "exploring space and planets seems impossible without the use of technologies based on Artificial Intelligence" [28]. The growing number of satellites in space and mission complexity have necessitated the development of technology to act upon unexpected events. To Feruglio, "the next generation of space missions will see software as the differentiating asset" [29].

In the context of space missions, the use of "AI on the edge", also known as edge computing or edge AI, involves computer programs and their data running on physical space objects, including satellites, to perform specific tasks. It is the application of software systems near the end user's location and consumption. This allows the space objects to process and analyze data at the generating source. Following Varma, data processing near its source reduces the issues associated with long-distance data transmission [30], reducing the latency between Earth and space-based assets.

3. Collection, processing, and sharing of data acquired in outer space

3.1. Introduction

The rapid development in the field of space exploration and technology is generating a large scale of data captured from outer space. The data collected ranges from remote sensing and telemetry to scientific research and communication-related information, all of which are necessary for operational efficiency, scientific advancements, and commercial ventures. Nonetheless, this data must be collected and processed effectively, which presents a major challenge to both management and security; along with the imperative to meet legal requirements.

Within the broader legal framework governing space activities, several provisions explicitly require states to share benefits, including scientific data, and to enhance international cooperation.

Notably, Article I of the Outer Space Treaty highlights that the exploration and use of outer space should benefit all countries, and Article IV of the Moon Agreement similarly calls for the sharing of benefits and information. However, the Moon Agreement has not received sufficient ratification to exert the influence originally envisaged.

More recently, the non-binding Artemis Accords (Section VIII) reiterate the importance of data-sharing among signatories. These instruments underscore a shared international commitment to ensuring that the benefits of space exploration are equitably distributed.

However, due to the complexity and essential nature of space data, a clear comprehension of collection, processing, and sharing mechanisms is needed. The desire for closer international cooperation and data sharing is increasing to a global level among space agencies, commercial organizations, and academia looking to achieve the maximum benefit from space exploration. The frameworks governing space data, including national regulations and privacy protection measures, are also shifting, making it essential to keep analyzing developments so as not to fall foul of intellectual property regulations or privacy protection.

Space data collection, processing, and transmission increasingly entertain the interaction of technologies such as AI, sensors, and communication systems. These technologies improve existing ways of obtaining and processing large volumes of data, giving meaning to otherwise baffling information and refining decision-making.

In space data processing, AI is employed to process Big Data to provide fast and precise analysis. Thus, it is possible to apply machine learning algorithms to pattern match and to find anomalous and trend-like structures in the data for a large number of use cases. For instance, satellite image analysis involves the use of AI algorithms in environmental surveillance, disaster identification, and land use planning. In this manner, AI facilitates the acceleration and optimization of data analysis, thereby enhancing the efficiency of space missions [31].

3.2. Importance of space data sharing across the international space community

The importance of data sharing cannot be overstated. Today, space exploration is an international collaborative endeavor, with several space organizations operating in concert. These agencies engage in a mutually beneficial symbiotic relationship, wherein they complement and reinforce each other's efforts by pooling human power, information, and ideas. Hence, through the coordinated cooperation of various entities, space exploration becomes more effective, and the study of space phenomena is enhanced.

Mars exploration missions such as NASA's Curiosity [32] and Perseverance [33] rovers, ESA's ExoMars [34] mission, and Indian Space Research Organisation (ISRO)'s Mars Orbiter Mission [35] have all played their part in throwing light on the red planet. In this way, the data collected and the information made available by these agencies contribute to painting the fullest picture possible about Mars. This can be used in future Mars missions, including human exploration. The exchange of data between these missions improves the quality and richness of scientific investigations of these phenomena.

Most of the questions and tasks connected with the challenges and opportunities of space exploration can only be addressed and resolved at the international level. This is because the sharing of data across different boundaries is usually a means of fostering trust and accountability, as well as a way of developing stronger understanding between individuals. This cooperative approach is especially needed in negotiating such matters as climate change, disaster preparedness and management, and resource utilization, among others that may come up from time to time.

Likewise, Copernicus Earth observation satellites "Sentinel-1" and "Sentinel-2" provide radar and optical imagery that can be utilized by the agricultural and urban development sectors [36,37]. This data is made available to users in accordance with the pertinent export control regulations, thereby facilitating international research and cooperation.

The commercial sector is also additive to gain a huge amount of advantage with the shared space data. Business organizations employ this data to create new diversified product and service solutions, capable of positively transforming the economy and effecting technological changes. Space data is applied in several commercial ventures, ranging from satellite telecommunication to Earth observation and navigation.

As evidenced by the endeavors of SpaceX and OneWeb, satellite data can be leveraged to bring Internet connectivity on a planetary scale through the deployment of mega-constellations in LEO, providing high-speed Internet access in regions otherwise lacking adequate infrastructure. The establishment of this common data infrastructure can effectively aid in overcoming the digital divide, thus, providing people from around the world with global accessibility to information and opportunities [38].

In the agricultural sector, private companies like Planet Labs and Satellogic beamed high-resolution images to farmers so that everyone learns of the best practices for maximizing yields while embracing sustainable farming practices. Such an example represents how space data does have commercial value and its diverse benefits to different industries on Earth [39].

3.3. Interoperability as a challenge in data processing

Processing data from space exploration missions is generally challenging. In particular, interoperability appears to be one of the most pressing needs when processing space data. Sharing and exchange of data across the different space agencies and institutions is often difficult due to the variety of different formats of data being used.

Interoperability is the characteristic that allows space systems and data formats to communicate with each other without problems. It is essential to the sharing and use of space data, which is why emphasis is being placed on this subject. There are a multitude of instruments and platforms for space missions that operate according to the work of various organizations, with different types of data formats and standards. Specifically, this diversity can make data integration and analysis arduous [40].

For example, the data from satellites used by NASA might be in a different format from the data obtained by ESA. Data from different sources must be in formats that are compatible enough to merge the datasets into a cohesive record. Some of the international organizations dealing with space data include the Committee on Earth Observation Satellites (CEOS) [41], which strives to develop standardization for space-recognized data. They promote 'open' data that can be shared and have more points of connection that boost the quality of data analysis [42].

Interoperability problems are also found in space communications systems. One major disadvantage is that every country and organization using radios has its own protocol and frequencies, which can interfere with each other or be significantly inefficient. These systems require to be coordinated on an international level, as well as through agreements that regulate the compatibility of the communication infrastructure. The creation of universal communication protocols improves the possibilities of inter-mission cooperation [43]. Interestingly, in Section V of the Artemis Accords a specific disposition is found on the importance of interoperability for space missions. As more states join the Accords, this provision has the potential to become a foundational tool for enhancing interoperability across the space sector.

3.4. Privacy and data protection

Privacy and data protection must be addressed in discussions regarding the management of space data. The monitoring and collection of information through space activities such as remote sensing and telemetry, along with the advent of new types of space objects, like mega-constellations of satellites in LEO, have given rise to concerns about data protection and security. Some examples include SpaceX's Starlink [44] and Amazon's Project Kuiper [45], the objective of which is to provide global internet services.

Despite the benefits their use brings to the advancement of worldwide connectivity, however, the deployment of these satellites on a large scale poses significant challenges to personal privacy [46]. Mega-constellations are capable of photographing and gathering information on nearly every point on the Earth's surface. While this functionality is useful in a variety of applications, it also brings about ethical dilemmas concerning the extent of monitoring and the continual and eternal surveillance they undertake over the Earth.

The fundamental tenets governing remote sensing were already prescribed in the 1986 Principles Relating to Remote Sensing of the Earth from Outer Space ("Remote Sensing Principles"). These principles underscore the openness of information and cooperation between countries conducting remote sensing transactions. Regarding the protection of individuals' privacy, they do not appear to be the proper instrument to resort to, as they are primarily focused on state interests rather than particular ones [47]. , The principles set forth herein do not make any reference, either implicit or explicit, to the human right to data protection in the event of images obtained through Earth observation remote sensing.

The question thus arises as to how the right to data protection can be protected in these scenarios. It is widely acknowledged that national regulations have always been considered one of the critical means for the protection of privacy in the context of space activities. Such legislation represents the sole means by which countries can regulate the methods of collection, processing, and storage of space data.

These laws should be capable of convergence with international norms, while simultaneously accounting for the specific national concerns [48]. Some examples include the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA); both of which would apply to the processing of personal data in outer space

[49].

Therefore, considering the risk of falling with the use of personal data, or at least the complication of completely opting out of the risk of laterally collecting personal data, therefore leaving an "ought to be a risk" to have personal data involved in the collection of data from space. It is of extreme importance to look at how the strict regulation regarding personal data, namely the GDPR, would interplay with space activities and AI. The GDPR regulates the collection, processing, and use of personal data of citizens of the European Union, irrespective of their location and/or registered domicile. It follows that companies handling data of European citizens outside of EU territory still must comply with GDPR dispositions.

Notwithstanding, we recognize that today there is no clear risk that space companies will have to deal with and comply with GDPR dispositions for their data collection from space, however, it is a problem that will be increasingly present in the coming years. Therefore, an initial analysis of which dispositions and limitations to bear in mind can be a long-term strategy to ensure the law-abiding dimension of their activities, in particolar in the context of remote sensing and earth observation. In particular, Article 22 can raise questions on services based on completely autonomous decision-making, banning decisions or systems that autonomously –without humans in the loop– make decisions.

As a result, satellites equipped with Very High-Resolution (VHR) cameras and an AI analytics software that autonomously discharges or sends data down to Earth could be impacted by it. Raising a bell given by the amount of fine that could be imposed by the breach of the GDPR, up to 20 million or 4 % of the undertaking's turnover. Yet in the same article, Article 22(3), a disposition is found that can help in the law-abiding building up of the services: "*The data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests*".

Specifically, safeguards can be placed following other core articles of the GDPR, such as Article 5 on the processing of data (data minimization & purpose limitation), Article 6 on the lawfulness of the processing (consent and/or legitimate interest), and lastly ensuring privacy by design and default according to Article 25.

It follows that these issues can only be addressed through the enactment of comprehensive legislation regulating the utilization of the given data and protecting the privacy rights of individuals. Moreover, certain measures should be taken by the representatives of the space industry concerning the protection of personal data. Such measures encompass the implementation of encryption systems, the utilization of secure communication protocols, and the adoption of robust access control mechanisms. It is also incumbent upon the managers of organizations involved in space activities to ensure that they conduct routine security assessments and risk/opportunity mapping.

3.5. The way forward in space data sharing: a multi-layered approach

This subsection shows that Space data-sharing in the age of AI demands particular attention. The stumbling block at the international law-making level does not diminish the clear need for more targeted guidance on AI-driven data usage in space.

One promising route can be presented by soft-law instruments, for instance, UN-endorsed guidelines or codes of conduct, that can flexibly adapt with technological development. These would build on existing ideals of benefit-sharing, cooperation, and transparency, but provide more practical standards for data handling, privacy safeguards, and interoperability. On a national level, governments could incorporate AI and data considerations into their licensing requirements for commercial spaceflight, thereby harmonizing practices across different jurisdictions and fostering de facto global norms.

Additionally, existing frameworks like the Artemis Accords, which already address data-sharing (section VIII) and interoperability (Section V), can be further refined or expanded to incorporate explicit AI governance and privacy protocols. While the Accords are not legally binding, their growing acceptance means they have real potential to influence behavior on a wide scale in the future.

All of this must go hand in hand with appropriate accountability measures. The foreseeable UN guidelines could possibly include the setting up of regular audits, establishing transparent oversight, and ensuring tangible avenues for redress would help protect fundamental rights while still encouraging innovation in space. In essence, rather than relying on a revision of the OST, a balanced and dynamic approach, mixing soft-law tools, coherent national regulations, and more robust use of existing frameworks (also from other fields, such as data protection) can provide the clarity and flexibility necessary for responsible AI-driven data processing in space activities in the years to come.

4. Cybersecurity of AI-enabled space systems

4.1. Introduction

As above-mentioned, AI is utilized across several domains [50]. However, a few issues have arisen concerning the use of AI to support Earth observation and monitoring efforts. These concerns are mostly related to employing AI-based solutions to meet cybersecurity and cyber defense goals in both military and civilian operations [51].

Cybersecurity is understood as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment, and organization and users' assets, including connected computer devices, and personal infrastructure [51].

AI, especially weak AI, is a cyber-vulnerable technology. A weak AI, otherwise referred to as narrow AI, is designed to perform specific tasks [52]. In addition to being susceptible to typical cyberattacks [53], AI systems –in particular, those that employ machine learning–, also rely on how AI functions and learns [54]. "Vulnerability" in AI cybersecurity refers to a flaw in the software, hardware, or operating systems while "risk" is the possibility of losing, harming, or destroying assets. In this way, attacks are possible against AI-enabled systems in space because the underlying AI algorithms have fundamental limitations that are now unfixable. They vary from conventional cyberattacks, which are brought on by "bugs" or unintentional coding errors made by developers in the source code [55].

Attacks can target weaknesses in the training process (e.g., data poisoning) or security in the training algorithm (e.g., adversarial machine learning). In addition, categorization outcomes may also be impacted by flaws in the platform on which the AI system operates. Examples include a higher-level qualitative study to reason about the impact of huge vulnerability classes on AI systems and a tangible proof-of-concept assault to demonstrate the viability and impact of a platform attack [55].

4.2. Legal framework for cybersecurity in space

Without sufficient engineering-phase verification and acceptance testing, using AI technology in space activities might be quite risky. As the use of AI-driven space systems is expanding rapidly, it is critical to keep the complexity and breadth of regulatory frameworks to protect these resources from cyberattacks. Satellites, spacecraft, and ground control infrastructure are all examples of space systems, which are becoming increasingly essential to international trade and national security. Thus, the implementation of strong, all-encompassing cybersecurity protocols is required based on the distinct attributes of space, such as its size, isolation, and the participation of several global parties.

When the five fundamental space treaties were adopted, neither cyberattacks nor emerging technologies (i.e., AI) were prevalent. At the time, it was unclear how these regulatory instruments would hold up to the harmful "activities/interferences" caused by new technologies. The well-known Roman legal adage *sic utere tuo ut alienum non laedas*, which

prescribes that each must use their property in a way that does not cause injury to another's, might serve as a starting point for understanding and debating potential developments in the fields of cybersecurity and space travel.

However, victims are left to navigate unknown territory due to the lack of established international law on AI, space, and cyberspace; as well as given the lack of distinctions between cybersecurity and space security, and the uses of technology. Accordingly, there is an increasing demand for cybersecurity rules addressed at both international and regional levels.

4.3. International space law

The OST can be seen as a seminal document for outer space law [56], which lays out important principles for the governance of space activities. Starting from the beginning, it is indicated in Article I OST that "the exploration and use of outer space shall be carried out for the benefit and in the interests of all countries". In the context of using AI systems in space activities, especially in autonomous operations, this provision may be interpreted as an obligation of states to ensure that these systems contribute to the collective benefit and do not lead to harmful monopolization or misuse.

Article VI OST holds "states responsible for national space activities, whether carried out by governmental or non-governmental entities". This responsibility extends to the cybersecurity of AI systems, as states must ensure that these systems do not pose risks to other states or entities. It should also be noted that the responsibility of states for space activities must be strictly differentiated from the liability of the state for damages caused by a space object according to Article VII OST and the LIAB, which builds on Article VII OST by defining a dual-pronged liability system based on fault and absolute culpability, depending on the location of the harm [57].

Article IX OST requires "states to avoid harmful contamination of space and adverse changes to Earth's environment." AI systems in space, especially those subject to cyber-attacks, could potentially cause harm (e.g., by disrupting satellite operations). States need to implement cybersecurity measures to comply with this obligation.

In conjunction with the aforementioned space treaties, given that the responsibility scheme accrues on the launching state of a space object, the launching state of an AI-enabled space object has been proposed as the suitable party to which liability should be traced back in the lack of better guidance. This suggests that all "intelligent" space systems launched from a state's territory must be authorized ex-ante and closely supervised; being the duty of the launching state to take all necessary precautions to lessen any possible harm their space objects may cause [58].

States may also be held accountable for not adequately protecting AI-enabled space objects from hacking, interruptions, or other security breaches that might jeopardize automated navigation and communications systems [3].

4.4. General international law

One of the fundamental principles of the OST is that international law applies to activities in space. Manfred Lachs, a founding father of the OST, wrote in 1972: "By accepting the Charter as part of contemporary law application to outer space and celestial bodies, one has to accept it as it is today, including all the progress made during the years it has been in operation" [59]. To this end, without a doubt, space is subject to a significant portion of international law. This covers both fundamental and explicit principles of international law as well as long-standing standards of customary international law, such as the *pacta sunt servanda* and good faith principles [55].

The 2001 International Law Commission's Draft articles on the Responsibility of States for Internationally Wrongful Acts aim to codify the customary law revolving around state responsibility [60]. According to the OST, along with cyber operations and other associated cyber activities, space activities are also subject to the law of state responsibility [61]. As per these Draft Articles, every internationally wrongful act, which includes both actions and omissions, which is committed by a state, consists of two components: (1) the attribution of the said wrongful act to the state in question under international law, and (2) the state's violation of an international duty [62].

In addition to these two components, it is important to determine whether there were any circumstances surrounding the alleged wrongfulness of the act [63]. When a state perpetrates an internationally unlawful act, it assumes international responsibility which has legal ramifications, such as the need to cease the behavior (if appropriate) and to provide full compensation for the harm caused [64].

In combination with the OST, Articles VI and VII do not affect any claim under customary international law on compensation. Article VII OST is not the only exclusive norm on compensation. The concept laid down by Articles VI and VII allows for liability of a launching state that is not (and never was) responsible in terms of Article VI, which never could commit a wrongful act in neglecting Article VI [55].

When it comes to AI systems in space, a cyber operation that violates an international regulation by targeting or using an AI system in a way that is traceable to a state, may be considered internationally unlawful conduct in accord with the Draft Articles. States may be held directly liable for cyber activities carried out by its branches, such as intelligence or the military.

States may also be indirectly held accountable if non-state actors, such as private companies or hacktivists, conduct cyberattacks while acting on behalf of the state or with its consent. Because cyber actions are sometimes anonymous and deniable, it is difficult to attribute an activity to a state in cyberspace. States could still be held accountable, though, if there is proof connecting the cyber operation to actions that are supported by the state.

In conclusion, under the current international law regime, it is not difficult to imagine if an AI-controlled spacecraft is compromised by a cyberattack, crashing into another satellite and producing debris that endangers other space assets. If a state is responsible for the attack, it may have violated the OST and perhaps triggered the LIAB, making it an internationally unlawful act.

Another scenario could be a violation of obligations under the International Telecommunication Union (ITU) regulations and the United Nations Cybercrime Convention, adopted on 7 August 2024, if a state conducts or sponsors a cyber operation that manipulates AI systems controlling critical satellite communications, causing widespread disruption of global communications, especially if the operation violates the principle of non-intervention.

4.5. Soft law

From a soft law perspective, guidelines for responsible space operations, with an emphasis on safety and debris mitigation, are provided by UNCOPUOS documents like the 2021 Long-Term Sustainability Guidelines [65] and the 2010 Space Debris Mitigation Guidelines [66]. In creating regulatory frameworks for space activities, including AI-based space systems, the Long-Term Sustainability Guidelines also promote the use of international technical standards.

Furthermore, it is noteworthy that the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE) in Tallinn was established more quickly than planned in 2007 because a number of Estonian public and private e-services were the targets of a wave of hostile cyber activities. As a result, governments all around the globe now use the Tallinn Manual as a reference for determining how international law should be applied in certain circumstances [67]. Although it is not a legally binding document, it is highly influential in shaping the understanding of how international law can be applied to cyberspace.

By designing and executing performance and safety standards, as well as conformity assessments for processes and products, international

standards organizations, such as the Institute of Electrical and Electronics Engineers (IEEE), and the International Organization for Standardization (ISO) are leveling the playing field between jurisdictions. These organizations are presently concentrating on standardizing AI by establishing committees specifically tasked with creating AI-related standards and assessment models.

In addition to releasing recommendations for AI management systems, ISO has established a Subcommittee on AI (SC42) to provide standards for the technical elements of AI development and conformity assessments [68]. Likewise, IEEE is developing AI standards, namely the Standard for Transparency of Autonomous Systems, on reliable AI, ethics, bias, and system quality [69].

Furthermore, several international organizations have released papers on ethical AI development. A worldwide agreement on the advancement of ethical AI has been adopted by the United Nations Educational, Scientific and Cultural Organization (UNESCO) 193 Member States [70], and the United Nations Chief Executives Board (UN CEB) has stressed the significance of ethical AI in its speech [71]. Additionally, 47 countries have embraced the robust, safe, fair, and trustworthy AI principles endorsed by the Organization for Economic Co-operation and Development (OECD) [72], whereas the World Economic Forum (WEF) has published a white paper on the public sector's procurement of reliable AI systems [73].

4.6. Proposed solutions and recommendations

4.6.1. State responsibility for cybersecurity of AI systems in space

The application of "cyber due diligence" can be viewed as one of the possibilities to promote international peace and security in outer space, within an unstable cyber environment, and to minimize dangers in the latter. If a state fails to pay due attention and care, as required by the specific activity-conduct-entity, it should be accountable for any inaction, whether it be generally or for the behavior of individuals [74].

According to the due diligence concept, nations must establish guidelines and policies to control and safeguard their cyberspace, cyber activity, and individuals involved in such activities. Therefore, states and companies need to comprehend and reinterpret the following concepts to properly manage space cybersecurity [75].

- "Harm" should be understood as taking into account the technique employed and the surrounding conditions.
- The probability and extent of the technology employed that contributed to the harm should be considered.
- The danger or known weaknesses in the technology and the environment in which it is employed should be examined.
- The degree of ex-post traceability and intelligibility of technological processes that might have had a role in the cause, as well as the asymmetry of information, should be understood.
- The level of ex-post accessibility and intelligibility of the information gathered and produced by technology should be reviewed.
- The type and extent of harm that may have been inflicted should be analyzed.

The liability is contingent upon the purpose of the offender or the operator's negligence, even in cases where the harm is produced or initiated by a cyberattack. In the absence of a legal framework, due diligence can be used to challenge broad expectations of reasonable care and consideration for threats to sovereignty between states [49].

In the case of cybersecurity for an AI-driven space object, numerous challenges arise regarding how to interpret and implement the identified subset of security measures. The concept of 'due attention and care' is particularly complex in this context, as the unique and evolving nature of AI makes it difficult to determine how these principles should manifest in specific scenarios. For instance, due diligence in the diffusion of AI within space operations could involve multiple aspects, such as ensuring the transparency of the model, clearly defining the mechanisms governing data sharing, and establishing robust safeguards to prevent unauthorized access or manipulation.

Additionally, addressing potential biases in AI decision-making and implementing continuous monitoring systems would be crucial to maintaining security and reliability. As AI increasingly integrates into space activities, a well-defined framework for cybersecurity and accountability will be essential to mitigate risks and ensure the safe and ethical deployment of these technologies.

4.6.2. The positive implementation of existing rules

Even though there is indeed a lack of international-level regulations on AI-driven space systems, it is challenging to negotiate new, internationally enforceable legal instruments given the international law-making stalemates. Under these conditions an incremental (or soft-law) approach may offer a concrete approach, which is likely to be the most effective way to reach some cohesive instrument in the matter.

In terms of substantive international commitment and norm creation, starting with non-binding non-governmental guidance documents informed by current and emerging industry initiatives, to then continue with the enforcement of these documents through national regulation, to ultimately negotiate binding international agreements. If adopted, this approach will grant the international community more time to suggest, discuss, and agree upon the current international space law framework.

This measurement is foreseeable also based on the practical side. In practice, insurance companies may ask prospective clients to produce comprehensive technical documents or compliance certifications, regardless of national regulations, to make sure that the risk of insuring them is low enough to warrant exposure to considerable liability in the case of a claim. This is particularly true in light of the growing likelihood of conjunction events occurring in orbit and the challenges insurance faces in sustaining successful business models as space debris multiplies [76].

5. Dual use of autonomous space assets

Traditionally, new space missions are dependent on data from previous studies, which can often be limited. In this regard, AI enhances satellite capabilities in mission design and planning by offering quick access to comprehensive data from past missions, allowing engineers to retrieve this information with just a few clicks. For instance, Daphne [77], an intelligent assistant, helps engineers in designing Earth observation satellite systems by providing relevant information and answering mission-related questions [78].

Moreover, AI technologies support navigation systems. The distance from Earth, Earth orbits, and planets are enormous, which could have a significant impact on the allocation of the spacecraft to its planned destination due to the challenge of the lack of a space navigation system. In matters of communication between Earth and satellites, which could cause enormous latency issues, with the risk of affecting the ability to avoid collisions [79]. AI opens the way to overcome these challenges: for example, there is the prospect of employing Intel and NASA's Intelligent Navigation System, which was built using images acquired by the Lunar Reconnaissance Orbiter, to generate a virtual lunar map [80].

In turn, AI technology offers a significant advantage in the enhancement of national defense through the integration of space assets. Several countries, namely the US, Russia and China, are already testing and integrating AI systems into existing defense systems to enhance intelligence and assessment capacity with further hope to even amplify the overall military command and control process [81].

To begin with, AI could be combined with traditional space intelligence, surveillance, and reconnaissance (ISR) space systems, improving tracking of adversary activities or assets on a larger scale over a longer period [82,83]. For instance, Slingshot Aerospace developed an AI system "Agatha" that analyzes maneuvering patterns of satellites in orbit and identifies anomalous activities that may be of potential security

interest. Under a contract with the US Defense Advanced Research Projects Agency (DARPA), Slingshot Aerospace developed the Agatha system and has run official tests including the tracking of Russia's Luch Olymp-K-2 inspector satellite [84].

Furthermore, AI could also be applied to assist in integrating cross-domain military command from data collection to weapons systems, envisioning the concept of Combined Joint All-Domain Command and Control (CJADC2). In June 2024, Lockheed Martin launched two demo satellites with three objectives of autonomous and collaborative data collection, tactical and over-the-horizon communication, and on-edge processing. One demonstration involves real-time collective data processing with an F-35 fighter jet and sending the processed information to the Aegis Combat System within a naval ship [85].

However, the dual-use nature of autonomous space assets powered by AI presents significant challenges. It necessitates both careful consideration and the establishment of comprehensive regulatory frameworks to ensure the responsible and ethical use of AI in space.

5.1. International norms on the dual-use of AI

5.1.1. Group of Governmental Experts on emerging technologies in Lethal Autonomous Weapons Systems (LAWS GGE)

In 2013, the Conference on the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons (CCW) convened the Group of Governmental Experts on emerging technologies in Lethal Autonomous Weapons Systems (LAWS GGE), mandating the group to conclude some guiding principles to draft proper regulation under the international law system.

Accordingly, in April 2021, eleven guiding principles and five protocols were adopted at the CCW conference, having affirmed the full application of the UN Charter and international humanitarian law [86]. While the guiding principles did not specify the exact accountability and type of crimes, states agreed to retain human responsibility for the decisions to use lethal autonomous weapons [87] and to comply with applicable international law on the potential development, acquisition, and use of those weapons [88].

5.1.2. Wassenaar Arrangement

The Wassenaar Arrangement on Export Controls for Convention Arms and Dual-Use Goods and Technologies (hereinafter, the Wassenaar Arrangement) was fully established in July 1996 to promote transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies [89].

As of today, 42 participating states are required to report their arms transfers, as well as to report every six months when they transfer or deny certain dual-use goods and technologies to destinations outside the Arrangement. Although participating states are not entitled to the right to veto or to make exemptions from the reporting obligation, the Arrangement does not include any penal clauses or sanctions for any actions against its provisions.

Regarding the dual-use list, when including items specific to telecommunications, sensors and lasers, navigation and avionics, aerospace and propulsion, all licenses denied relevant to the purposes of the Arrangement should be notified by participating states to non-participants twice a year [90]. Moreover, participating states must biannually notify licenses issued or transfers of items in the Sensitive List and Very Sensitive List made relevant to the purposes of the Arrangement to non-participating states [91].

Most of the items listed under the Arrangement are highly prone to military applications and are thus defined as dual-use items. In that sense, autonomous space assets would also easily fall under the dual-use items as long as the original technological application is included in the list. For instance, autonomous navigation systems for space launch and maneuver will fall under the term "source code" for "the operation or maintenance of any inertial navigation equipment, including inertial equipment, or Attitude and Heading Reference Systems (AHRS)" that are specifically advanced as listed under the Arrangement [92].

Also, other source codes for "hybrid integrated systems which improve the operational performance or reduce the navigational error of systems" to the specified level combining sonar velocity data, satellite navigation reference data, or Data-Based Referenced Navigation (DBRN) systems are regulated under the Arrangement [93].

5.2. Regional rules and policies

Leading states in AI development and domestic regulations have started to propose the potential risks and governance of AI as an EDT, introducing it as an official item on the agenda at both regional and multilateral levels. This term has been coined by several governments and relevant industry actors, increasingly receiving critical attention at the European Union (EU) and the North Atlantic Treaty Organization (NATO).

Under the term, AI may be technologically neutral and its use would not itself harm people, but the military application of the technology to automatically target and attack would be disruptive. In that sense, the 2021 meeting of NATO Ministers of Defence –concluded with a joint NATO Artificial Intelligence Strategy– led to the formulation of six principles of responsible use of AI in defense: (a) lawfulness, (b) responsibility and accountability, (c) explainability and traceability, (d) reliability, (e) governability, and (f) bias mitigation [94].

Moreover, the European Commission convened a High-Level Expert Group on AI to address issues and derive common objectives within Europe concerning ethical development, deployment, and use of AI. As a result, in April 2019, the European Commission published its "Ethics Guidelines for Trustworthy Artificial Intelligence" [95], containing seven key requirements that AI systems should meet to be deemed trustworthy: (a) human agency and oversight, (b) technical robustness and safety, (c) privacy and data governance, (d) transparency, (e) diversity, non-discrimination and fairness, (f) societal and environmental well-being, and (g) accountability.

Such principles formulated the ethical basis on which the 2024 EU's AI Act would later be based, considered as the first-ever comprehensive regulatory framework regulating the use of AI. Nonetheless, this legislation excludes AI systems used for military, defense, or national security purposes from its scope (Art. 2), as the GDPR does, therefore leaving open questions on the nature of dual-use assets, including space systems.

In May 2024, the Council of Europe passed its Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law' to provide guiding principles and necessary procedures for all actors to comply with the existing standards on human rights, democracy, and the rule of law [96]. The Convention stipulates seven principles [97], following appropriate remedies, procedural rights, and safeguards for states and private actors. Notably, the Convention obliges state parties to either comply with the principles and obligations or take other measures to comply with the treaty provisions while fully respecting their international obligations regarding human rights, democracy, and the rule of law.

Meanwhile, parties to the Convention are exempted from treaty obligations when conducting activities related to the protection of their national security interests and national defense matters [98]. However, state parties are not exempted from treaty obligations even in the case of national security interest, when the testing of AI systems may have the potential to interfere with human rights, democracy, or the rule of law [99].

5.3. Legal challenges related to the dual-use of AI in outer space

Albeit there are several existing international rules and guidelines applicable to space activity and AI use, respectively, the application of AI technologies in outer space and its dual-use character poses a series of regulatory and political challenges.

Firstly, the application of AI in space launches and maneuvers

complicates state liability under international law and, specifically, under the LIAB. For instance, the LIAB only defines the term 'launching state' as a state that launches or procures the launching of a space object or a state from whose territory or facility a space object is launched [100]. The Convention, unfortunately, does not delimit in detail the launch or procurement itself and cannot thus specify how and where the party that provides an AI-driven or AI-supported launch and maneuver system fits in the legal equation.

Any damage caused by one state party to another by using an AI-powered dual-use space object does not exempt the state party from its liability. However, further liability of the AI software-providing or operating state would be subject to the problem of causation and proof, thus lacking effective and appropriate rules regarding the level of autonomy and burden of proof [101].

Secondly, the absence of any binding regulations on AI applied to space systems will lead to allowing any dual use of the technology, from autonomous reconnaissance to even lethal autonomous weapons, which would be contradictory to the principles of peaceful use and non-militarization of outer space under the OST, and to the general prohibition of threat or use of force under the UN Charter.

While the above-suggested guiding principles from UN expert groups and even NATO joint ministerial documents highlight the need to retain human responsibility and accountability in using AI, both documents curtail the scope of defense applications and do not initially call for regulatory tools on the disruptive use of AI in space. In such cases, states and private actors will only consider general interpretations of international law and, in the case of the use of force, humanitarian law. While these may not be in contradiction with the international rules-based order, they may undermine the very purpose of peaceful use and regulation, including the non-placement of weapons of mass destruction in accordance with the OST.

Thirdly, the application of autonomous systems into lethal weapons potentially raises the risk of human control in decision-making and further breach of international humanitarian law when executed. Increasing views from academia and the international community criticized the danger of fully autonomous weapons deployed based on pre-designed algorithms and without any human control [102–104].

Some have also argued from an international law perspective that the use of AI technology complicates the problem of command and chain of responsibility, although it will remain challenging to clarify the extent of law permitting, requiring, and prohibiting lethal autonomous weapons [105]. In particular, legal questions could be raised under international humanitarian law on whether autonomous weapon systems still comply with the four core principles of distinction, necessity, humanity, and proportionality just like any other weapons.

6. Intellectual property rights in AI application

With the use of AI in space technology, new challenges might arise regarding Intellectual Property Rights (IPRs). IPRs are rights that protect an innovative thought, depending on its form [106]. International treaties and Intellectual Property (IP) regimes identify six different IPRs, namely patents [107], copyrights [108], trademarks [109], industrial designs [110], geographical indications [111], and trade secrets [112].

From the perspective of IP, the most important application of AI within the space domain appears to be in the field of imaging. To evaluate the potential legal implications and regulatory challenges of AI in space, it is essential to first understand how AI is being embedded into space technology. This integration can be examined in three key areas: the AI deployment on Earth, the use of AI systems in space, and the outcome of the latter on Earth or in space.

From a legal standpoint, it is crucial to differentiate between the input to AI models and their output. This has particular relevance for the applicability of international space law and intellectual property law.

6.1. Input to AI models

Input data to AI, in EU terms, refers to "data provided to or directly acquired by an AI system based on which the system produces an output" [113] and can be introduced to the AI in different states such as raw, cleaned, organized, or labeled data [114]. Firstly, it is necessary to understand that AI models are, in the vast majority, being developed on Earth [115]. This does limit the applicability of international space law. However, several intellectual property law aspects can be recognized at this stage.

i. *Stages of AI and machine learning development*

AI model development can be divided into four phases: (i) setup phase, (ii) model training phase, (iii) models exploitation phase, and (iv) deployment phase [116].

To begin with, the setup phase is described by data collection, methodology such as annotation protocol for performance of annotation tasks, metadata tags (labels) for data annotation, and structured label taxonomy; all of them being eligible for protection under copyright [116]. This means that after identifying a problem that needs to be solved by AI, the proper data is collected and sorted for the upcoming training [117].

The model training phase consists of entire metadata labels and corresponding data samples (labels metadata), machine learning models, and active learning flow (algorithm) [116]. This stage plays a key role in a successful outcome in the long run - understanding the data, labels, and other sources from the previous phase helps with the proper design and calibration of the machine learning model in order to achieve the best results for the aimed goal with the available input [118]. In this case, these data can be protected under copyright, but also under trade secrets and patents [116].

The model's exploitation phase can be described by pipeline data flooding for desired output (machine learning output), interference software interface, data processing through machine learning pipelines, and training software interface like source code [116]. This means that the developer tries to secure the best outcome out of the data by using algorithms or previously learned policies in a short period [119]. While machine learning output is inherently hard to protect, the remainder can be adequately safeguarded through the use of copyrights and patents [116].

Lastly, the deployment phase of AI in IP consists of web application software, software interface providing service to other pieces of software, machine learning software libraries of third parties, edge applications, and deployment infrastructure; which can be protected by patents and copyrights [116]. This includes taking into account integrating the AI model into the targeted application, feedback, and updates as well as incorporating security measures [120].

In a nutshell, the development of AI involves preparing for the AI project by first defining the goal and gathering as well as organizing relevant data. Further, it is dependent on choosing or creating a model, training it with the data, testing as well as fine-tuning the model, and finally deploying it for real-world use.

ii. *IP protection of training data*

As described, most of the AI training and development content can be protected under several IP protection mechanisms. Nonetheless, a legal question remains open, especially regarding ownership of training data within the setup phase, which then flows into the machine learning models in the next machine learning and AI development stages.

When Earth imaging is taken into consideration from the perspective of copyright, the training data as input for machine learning needs to be examined closely. At this stage, most input would be eligible for copyright protection. Nonetheless, as stated above, certain raw data are not copyrightable [121]. Therefore, training machine learning on raw data

would not be considered a breach of IPRs. If, however, machine learning is being trained with processed data such as images that are protectable under copyright [122], then this issue needs to be addressed.

Although several space agencies provide open-access datasets for machine learning and AI training [123,124], it is questionable to what extent legal challenges may arise. With the rise of AI applications, the question as to whether using copyrighted data for machine learning and AI training purposes constitutes an infringement is currently being discussed in many jurisdictions and various contexts. One approach is aligned with the idea established within the US copyright law that even copyrighted data can be used as training data for machine learning and AI under the fair use doctrine [121]. This means that the copyrighted data can be used when the purpose, the nature, and the effect on the market, are aligned with the fair use doctrine [125].

Further, especially when considering the use of data gained from private entities, licensing [126] is one of the other means of legally using data for machine learning and AI training purposes [121]. Also, data scraping is another way of using data for training purposes, although possibly leading to legal concerns [127]. Lastly, the data input might be constituted as a non-infringing protected derivative [128] by the so-called "transformative use" [122].

It is important to highlight that the higher the quality of the data, the better the AI output [129]. The debate around AI and IP includes also the fact that space applications of high quality can help solve, identify, and handle problems which oftentimes corresponds with the UN's Sustainable Development Goals (SDGs) [124].

6.2. Output of AI models

Firstly, it needs to be stated that an AI model is not the same as an algorithm, since the "model is used to make predictions or decisions and an algorithm is the logic by which that AI model operates" [130]. The output of AI models therefore depends on the input and the model, so the output is not necessarily an image just because the input was an image [131]. This is for the reason that "an AI model is defined by its ability to autonomously make decisions or predictions, rather than simulate human intelligence," which can be performed in other forms (for example, in text form) than the original input for training [130].

i. *From data to image*

Before AI systems were being implemented onboard space objects, amounts of space data would flow to a receiver on Earth (ground segment), and there, these would be processed into an image, that is, an IP-protectable outcome under national laws [132]. However, it must be pointed out that this matter, including copyright issues, may, and usually would, be handled by contracts and license agreements [133].

With AI being used in outer space technology, the situation slightly changes. Regarding Earth imaging, in particular, AI has become an invaluable aid, especially in terms of reducing data flows to Earth, and reducing the use of precious bandwidth [15]. This is enabled by AI identifying certain relevance within the data gathered in outer space and sending it back to Earth. There is a thin layer between the applicability of "earthly" jurisdictions, i.e. remaining status quo, and a new legal challenge.

ii. *Legal challenges*

In scenario one, AI in outer space would be processing only unprocessed, raw data [134]. It is to be noted that raw data is not subject to copyright and therefore cannot be protected at this stage [135]. If, conversely, data would be processed directly in outer space having (possibly) an image as the output –developed and existing in outer space–, the latter would be subject to copyright when fulfilling the definition of copyright as stated above.

The use of AI presents several legal challenges when applying IPRs on Earth and consequently, in the outer space domain. The issue of authorship is of particular relevance to the use of AI in space for its role in determining territorial jurisdiction. Especially, copyrightability of outputs of generative AI has been part of recent discussions all around the world, with most countries denying such IP protection due to a missing human involvement in the output [136]. It is also relevant to note that copyright is connected to the nationality of the author [137] and under the Berne Convention, TRIPS and WCT there is a certain level of protection of the copyrighted work in every signatory country, although the work itself might originate in another country [138,139]. Therefore, wherever used, copyright law would apply, since no registration is needed, but only within territories of the signatory states [140].

It is mandatory to mention that outer space is not a territory in terms of intellectual property rights protection and, therefore, only national laws regarding "earthly" territories or other acknowledged regimes can apply [141]. Space is not a territory in the sense of IP and therefore is not protected as such in outer space [142,143]. Although there is a separate legal regime concerning IP on board the International Space Station (ISS), this shall not apply to copyright [142].

An innovative idea made by AI in space would not be eligible for patent protection since only a human can be the founder of a patent [144]. In the United States, legal authorities have emphasized that AI cannot function as a "person" under copyright and patent law. Indeed, the United States Copyright Office (USCO) denied an application for a work produced with an AI system because the work was made "without any creative contribution from a human actor" [145]. This suggests that at least in the United States, the issue of "who" may qualify as an author for the purposes of IPRs appears to be relatively settled.

However, there is still debate as to whether AI-generated products or works may be granted protection. Even if the AI output was –in now more than rare cases– copyrightable, legal challenges would arise when the location of publication is outer space [142]. As applied to outer space, the extent to which intellectual property rights may be employed for AI systems in outer space must first contend with the territoriality of IPR and the non-appropriation principles (non-territoriality) [146] of outer space governance. Also, only the USA has, so far, extended its IP laws to registered space objects launched from its territory [147]. Nonetheless, the "doctrines of choice of law and national treatment, as governed by the Berne Convention, will be great legal resources in determining matters of copyright infringement related to space activities" [142].

6.3. The intersection of intellectual property law and international space law

Article I(1) and (2) OST prohibit the appropriation of outer space and emphasize that the exploration of outer space should remain an effort from which all of humankind may profit. Taken from an intellectual property rights perspective, this would mean that any claim of intellectual property monopoly including patents, copyrights, and trademarks, for an invention obtained through scientific experiments would be denied based on international law, despite the protection of intellectual property rights relying primarily on individual state enforcement [148].

Nevertheless, both Article VI and Article VIII present concepts that may be applied as a quasi-extension of national territory to extend intellectual property rights to AI systems in outer space. The former holds states directly responsible for the actions of non-governmental entities in outer space, so long as those activities are "national" in nature. This implies, as argued by Wedenig, that the development of specialized AI (narrow AI) intended for use in outer space should qualify as a national activity [23]. Additionally, the latter foresees that a state party to the treaty on whose registry an object launched into outer space is carried shall retain jurisdiction and control over such an object. In other words, Article VIII can be employed to indirectly permit the protection of

intellectual property rights in outer space [148].

The 1976 Registration Convention (REG) is also another mechanism by which national territory may be extended (via quasi-extension) to apply the protection of intellectual property rights. As such, a state of registry must maintain jurisdiction and control over the space object, as provided for by the OST [148]. In this regard, it should be noted that ownership not only covers the satellite and space station, but can also extend to include the launch vehicle, related stages and components, and payload, as well.

Both the OST and the REG provide a framework for the quasi-extension of national territory to outer space as a mechanism to apply the protection of intellectual property rights. The 1998 Intergovernmental Agreement on Space Station Cooperation (IGA) is perhaps the only legal regime that specifically addresses intellectual property rights in outer space; however, it is strictly limited to such use on the ISS.

Article 21 states that activity occurring in or on a space station flight element is deemed to have occurred only in the territory of the partner state of that element's registry. For example, for ESA-registered elements, any European partner may deem the activity to have occurred within its territory. The IGA also touches on the concept of temporary presence (parts or articles passing through a country on Earth or on their way to or from the space station); alone is not to be the basis for any intellectual property right infringement proceeding [149].

Insofar as how space data processed by AI systems onboard satellites may be protected by intellectual property law, the key factor in this determination is the critical link between jurisdiction and the type of AI data. In other words, whoever owns the AI-processed data is the one who retains the right to legally protect it. After identifying the relevant intellectual property law and which individual may claim ownership, we may apply extraterritorial jurisdiction of the state of which the individual is bound using international law.

In sum, reconciling the non-appropriation principle of outer space with the principle of territoriality enshrined in intellectual property rights protection regimes may be accomplished through the extension (quasi-extension) of national territory into outer space using the concept of registration, as outlined in the OST and the REG, and be guided by international treaties with articles designed specifically to address intellectual property right protection such as the IGA.

7. Conclusions

As highlighted in the introduction, the space industry stands at a crossroad, with the expanding integration of AI in orbit. The analysis in this paper has underscored how such integration holds immense benefits under different aspects. From mission efficiency, data processing, and deep space exploration, however, also give rise to new legal and policy questions.

The existing treaties, most notably the OST, offer core principles that can be read to include aspects of AI-driven missions, but fail to address pressing new challenges with sufficient specificity.

In particular, new layers of complexity open in space law in areas such as data-sharing, cybersecurity, dual-use governance, and IP. Although an amendment of the OST might appear tempting, its foundational role and the difficulty of achieving global consensus make such an approach both unlikely and potentially destabilizing to the broader space law framework. Instead, the space community should incrementally take concrete steps that build on existing principles while addressing the realities of AI-driven space activities, with a multi-layered approach. Rather than proposing an entirely new treaty or forcing amendments into the OST, the paper emphasizes an approach founded in both soft-law development and revision to national legislation. The harmonization of guidelines and the reinforcement of industry-led standards can offer an achievable path forward. Doing so it will ensure legal certainty to operators while still allowing for innovation. Such steps, if coordinated on a global level, can evolve into recognized best practices that pave the way to regulation at the international level if and when a stronger consensus emerges.

In particular, in relation to the areas analyzed in this paper some specific recommendations emerge. One of the most vital tasks is to encourage cross-sector collaboration among regulatory bodies, industry actors, and academic institutions, aiming to establish norms and best practices for data-sharing. Drawing lessons from other technological domains and ensuring that coherent data sets are used to train AI systems will support safer, more reliable mission outcomes and uphold privacy rights.

As space operations rely more heavily on automation, robust cybersecurity standards become indispensable. Threats like adversarial attacks, data corruption, and software vulnerabilities bring serious risks, not only to commercial activities and satellite constellations, but also to deep-space missions where timely human intervention may be limited.

Moreover, there is an increasing need of clarifying dual-use governance in the context of AI. Governments and international organizations must grapple with systems that can be applied equally to civilian and military ends, balancing the Outer Space Treaty's commitment to peaceful purposes with the realities of modern technological innovation.

In tandem, a revision of IP regimes for AI-driven activities, especially concerning ownership rights in outer space, remains necessary as machine-generated outputs and autonomous operations fall outside traditional legal categories.

In conclusion, there is no doubt that continued research and dialogue are essential if space law is to keep pace with the advancement of AI. The paper focused on data governance, cybersecurity, dual-use, and IP, to be able to craft targeted, practical solutions that address such novel issues while still preserving the broad principles of international space law. Over time, these multi-layered initiatives, whether enacted through soft-law instruments, national regulations, or expanded international accords, can offer the legal certainty, ethical grounding, and technical rigor needed to ensure that AI in space not only thrives but does so responsibly.

CRediT authorship contribution statement

Giovanni Tricco: Writing – review & editing, Writing – original draft, Supervision, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Roser Almenar:** Writing – review & editing, Writing – original draft, Supervision, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Kaili Ayers:** Writing – original draft. **Rihab Ben Moussa:** Writing – original draft. **Thomas Graham:** Writing – review & editing. **Simisola Iyiola:** Writing – original draft. **Sanghoon Lee:** Writing – original draft. **Terezie Němcová:** Writing – original draft. **Asiimwe Joshua Opota:** Writing – original draft. **Tushar Sharma:** Writing – original draft. **Raelee Toh:** Writing – original draft. **Jieyu Yuan:** Writing – original draft.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This research has been conducted by the members of the Space Law and Policy Project Group (SLP PG) of the Space Generation Advisory Council (SGAC), under the direction of Roser Almenar and Giovanni Tricco. The SLP PG has provided a valuable platform and support, guiding the development of this work and overseeing the project from its inception. Consequently, the team would like to acknowledge the SLP PG's Research Coordinators, Angelika Pizarro and Pankaj Mehta, as well as the SLP PG's Co-Leads, David Eagleson and Alvaro Piris.

References

[1] H.K. Athanasopoulos, Space 2040: the future of the global space economy. https://2bahead.com/downloads/space-2040, June 2023 accessed 20.09.24.
[2] ESA, Artificial intelligence behind 21st Century spaceflight. https://www.esa.int/Enabling_Support/Operations/Artificial_intelligence_behind_21st_Century_spaceflight, 28 January 2021 accessed 20.09.24.
[3] A.-S. Martin, S. Freeland, The advent of artificial intelligence in space activities: new legal challenges, Space Policy 55 (2021) 1–10, https://doi.org/10.1016/j.spacepol.2020.101408.
[4] M. Grobelnik, K. Perset, S. Russell, What is AI? Can you make a clear distinction between AI and non-AI systems?. https://oecd.ai/en/wonk/definition, 6 March 2024 accessed 20.09.24.
[5] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401689 (accessed 20.09.24).
[6] C. Stryker, E. Kavlakoglu, What is AI?. https://www.ibm.com/topics/artificial-intelligence, 2024 accessed 20.09.24.
[7] S. Brown, Machine learning, explained. https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained, 21 April 2021 accessed 20.09.24.
[8] McKinsey & Company, What is deep learning?. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-deep-learning, 30 April 2024 accessed 20.09.24.
[9] ESA, Artificial intelligence in space. https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Discovery_and_Preparation/Artificial_intelligence_in_space, 3 August 2023 accessed 20.09.24.
[10] R. Elite, Trends and Applications of AI in Space, https://interactive.satellitetoday.com/trends-and-applications-of-ai-in-space/(accessed 20.09.24).
[11] Space Inria, Inria and CNES join forces to build the satellites of the future. https://www.inria.fr/en/partership-inria-cnes-satellites-future-spaces, 8 April 2024 accessed 20.09.24.
[12] NASA Earth Data, Artificial Intelligence (AI), https://www.earthdata.nasa.gov/technology/artificial-intelligence-ai (accessed 20.09.24).
[13] P. Maguire, AI at the crossroads of cybersecurity, space and national security in the digital age. https://spacenews.com/ai-crossroads-cybersecurity-space-national-security-digital-age/#:~:text=SpaceX%20uses%20an%20AI%20autopilot,pioneers%20could%20only%20have%20imagined, 3 April 2024 accessed 20.09.24.
[14] Hogan Lovells, Artificial Intelligence and your space business: a guide for smart navigation of the challenges ahead. https://www.hoganlovells.com/~/media/ai-article-space-09nl.pdf, February 2018 accessed 20.09.24.
[15] NASA Science Editorial Team, New AI algorithms streamline data processing for space-based instruments, in: https://science.nasa.gov/science-research/science-enabling-technology/new-ai-algorithms-streamline-data-processing-for-space-based-instruments/, 20 December 2022 accessed 20.09.24.
[16] NASA, NASA Technology Roadmaps – TA 4, Robotics and autonomous systems. https://www.nasa.gov/wp-content/uploads/2016/08/2015_nasa_technology_roadmaps_ta_4_robotics_and_autonomous_systems_final.pdf, July 2015 accessed 20.09.24.
[17] J. O'Callaghan, This AI robot chemist could make oxygen on Mars. https://www.nature.com/articles/d41586-023-03522-4, 2023 accessed 20.09.24.
[18] ESA, Artificial intelligence boosts science from Mars. https://www.esa.int/Enabling_Support/Operations/Artificial_intelligence_boosts_science_from_Mars, 29 April 2008 accessed 20.09.24.
[19] Z. Royster, D. Logsdon, AI has the power to change the future of space. https://www.itic.org/news-events/techwonk-blog/ai-has-the-power-to-change-the-future-of-space, 2023 accessed 20.09.24.
[20] D. Li, Cyber-attacks on space activities: revisiting the responsibility regime of article VI of the outer space treaty, Space Policy 63 (2023) 1–13, https://doi.org/10.1016/j.spacepol.2022.101522.
[21] Treaty on principles governing the activities of states in the exploration and use of outer space, including the Moon and other celestial bodies (outer space treaty). https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html, 1967.
[22] Convention on International Liability for Damage Caused by Space Objects, Liability Convention), 1972. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introliability-convention.html.
[23] S.-M. Wedenig, Artificial intelligence in outer space: the responsibility of the state of the software developer. https://www.mcgill.ca/iasl/article/artificial-intelligence-outer-space-responsibility-state-software-developer, 2023 accessed 20.09.24.
[24] J. Eickhoff, Onboard Computers, Onboard Software and Satellite Operations: an Introduction, Springer, Berlin, 2012, https://doi.org/10.1007/978-3-642-25170-2.
[25] S. Chien, et al., The future of AI in space, IEEE Intell. Syst. 21 (4) (2006) 64–69, https://doi.org/10.1109/MIS.2006.79.
[26] A.A. Omar, M.M. Farag, R.A. Alhamad, Artificial Intelligence: New Paradigm in Deep Space Exploration, 14th International Conference on Developments in eSystems Engineering (DeSE), University of Sharjah, United Arab Emirates, 2021, pp. 7–10, https://doi.org/10.1109/DeSE54285.2021.9719425. December.
[27] P.A. Oche, G.A. Ewa, N. Ibekwe, Applications and challenges of artificial intelligence in space missions, IEEE Access 12 (2024) 44481–44509, https://doi.org/10.1109/ACCESS.2021.3132500.
[28] P. Pant et al., AI based technologies for international space station and space data, 11th International Conference on System Modeling & Advancement in Research Trends (SMART), Moradabad, India, 2022, 16 – 17 December. DOI: 10.1109/SMART55829.2022.10046956.
[29] L. Feruglio, et al., Future-ready space missions enabled by end-to-end AI adoption, in: M. Madi, O. Sokolova (Eds.), Artificial Intelligence for Space: AI4SPACE – Trends, Applications, and Perspectives, CRC Press, Boca Raton, 2024, pp. 303–360.
[30] M. Verma, Edge computing in space: enhancing data processing and communication for space missions, International Journal of Trend in Scientific Research and Development (IJTSRD) 8 (1) (2024) 1041–1045. Available at: https://www.ijtsrd.com/papers/ijtsrd64541.pdf.
[31] https://sensorpartners.com/en/knowledge-base/artificial-intelligenc-and-sensors-a-powerful-combination/(accessed 20.09.24).
[32] https://science.nasa.gov/mission/msl-curiosity/(accessed 20.09.24).
[33] https://science.nasa.gov/mission/mars-2020-perseverance/(accessed 20.09.24).
[34] https://www.esa.int/Science_Exploration/Human_and_Robotic_Exploration/Exploration/ExoMars (accessed 20.09.24).
[35] https://www.isro.gov.in/MarsOrbiterMissionSpacecraft.html (accessed 20.09.24).
[36] https://sentinels.copernicus.eu/web/sentinel/copernicus (accessed 20.09.24).
[37] K. Amankulova, et al., Integrating the Sentinel-1, Sentinel-2 and topographic data into soybean yield modelling using machine learning, Adv. Space Res. 73 (8) (2024) 4052–4066, https://doi.org/10.1016/j.asr.2024.01.040.
[38] G. Tricco, The upcoming of Iris2: bridging the digital divide and strengthening the role of the EU in International Space Law, Journal of Law, Market & Innovation 2 (2) (2023) 17–42, https://doi.org/10.13135/2785-7867/7952.
[39] G. Rausser, E. Choi, A. Bayen, Public-private partnerships in fostering outer space innovations, Proc. Natl. Acad. Sci. USA 120 (43) (2023) 1–10, https://doi.org/10.1073/pnas.2222013120.
[40] S. Lewis, Interoperability, December 2023, https://www.techtarget.com/searchapparchitecture/definition/interoperability (accessed 20.09.24).
[41] https://ceos.org/about-ceos/overview/(accessed 20.09.24).
[42] ESA, Newcomers Earth Observation Guide, 11 August 2020, https://business.esa.int/newcomers-earth-observation-guide (accessed 20.09.24).
[43] A. Salmeri, One size to fit them all: interoperability, the Artemis accords and the future of space exploration. https://spacewatch.global/2020/11/spacewatchgl-opinion-one-size-to-fit-them-all-interoperability-the-artemis-accords-and-the-future-of-space-exploration/, 2020 accessed 20.09.24.
[44] https://www.starlink.com/(accessed 20.09.24).
[45] https://www.aboutamazon.com/what-we-do/devices-services/project-kuiper (accessed 20.09.24).
[46] T. Kohnstamm, Everything you need to know about Project Kuiper, Amazon's satellite broadband network. https://www.aboutamazon.com/news/innovation-at-amazon/what-is-amazon-project-kuiper, 2024 accessed 20.09.24.
[47] F.G. von der Dunk, Outer space law principles and privacy, in: D. Leung, R. Purdy (Eds.), Evidence from Earth Observation Satellites: Emerging Legal Issues, Brill, Leiden, 2013, pp. 243–258. https://digitalcommons.unl.edu/spacelaw/96.
[48] https://www.britannica.com/event/Outer-Space-Treaty (accessed 20.09.24).
[49] M.M. Zoltick, J.L. Colgate, The application of data protection laws in (outer) space, in: International Comparative Legal Guide to: Data Protection 2019, Global Legal Group Ltd., 2019, pp. 6–11. https://www.rothwellfigg.com/assets/htmldocuments/ICLG_Data_Protection_2019_RothwellFigg_Outer_Space.pdf.
[50] I. Serrano, How artificial intelligence is advancing space efforts. https://www.geospatialworld.net/prime/technology-and-innovation/how-artificial-intelligence-is-advancing-space-efforts/#:~:text=Scientists%20use%20AI%20to%20control,communication%20between%20Earth%20and%20space, 20 April 2023 accessed 20.09.24.
[51] A. Carlo, et al., The importance of cybersecurity frameworks to regulate emergent AI technologies for space applications, Journal of Space Safety Engineering 10 (4) (2023) 474–482, https://doi.org/10.1016/j.jsse.2023.08.002.
[52] A weak AI, also called narrow AI, is capable of performing a specific task that its designed to do. See https://builtin.com/artificial-intelligence/strong-ai-weak-ai (accessed 20.09.24).
[53] Substantial research has been devised to assess and challenge the security of AI and ML models. Numerous attacks have been designed to expose the vulnerability of AI systems. These attacks can impact all the phases of the ML lifecycle. For instance, some attacks have been designed to affect the training phase. This may include 'poisoning attacks' and 'backdoor attacks' when the training data are intentionally altered to hinder the model's learning process. Similarly, during the testing phase, the probability of 'evasion attacks' increases when the input data are modified to deceive the model during inference and alter the prediction of the AI system, usually by introducing minor and imperceptible alterations (adversarial attacks). Attacks can also be classified according to the adversary's goal. Those that aim to diminish the effectiveness or detection performance of the ML model are described as questioning the model's integrity. On the other hand, those that aim to recover private or confidential data embedded into the model or the training set are described as confidential or privacy attacks, e.g. model stealing, model inversion and membership inference". See J. Martinez del Rincon et al., Study of Research and Guidance on the Cyber Security of AI, Centre for Secure Information Technologies (CSIT), Queen's University Belfast (QUB), United Kingdom, pp. 1–24. https://assets.publishing.service.gov.uk/media/663cf1b2bd01f5ed3279388e/Study_of_research_and_guidance_on_the_cyber_security_of_AI_-_Queens_University_Belfast_literature_review.pdf.
[54] L. Pupillo, et al., Artificial intelligence and cybersecurity: technology, governance and policy challenges task force evaluation of the HLEG trustworthy AI

assessment list (pilot version), CEPS Task Force Report (22 January 2020). http://aei.pitt.edu/102463/.
[55] A.H. Kim, The Impact of Platform Vulnerabilities in AI Systems, Massachusetts Institute of Technology, 2020. Ph.D. Dissertation, https://dspace.mit.edu/handle/1721.1/129159.
[56] A. Pytlak, J. Siebens (Eds.), Advancing Accountability in Cyberspace: Models, Mechanisms, and Multistakeholder Approaches, STIMSON, July 2024. https://www.stimson.org/2024/advancing-accountability-in-cyberspace/.
[57] V. Gupta, Critique of the international law on protection of the outer space environment, Astropolitics 14 (1) (2016) 20–43, https://doi.org/10.1080/14777622.2016.1148462.
[58] G.A. Gal, et al., Artificial intelligence in space. https://doi.org/10.48550/arXiv.2006.12362, 22 June 2020 accessed 20.09.24.
[59] M. Lachs, The Law of Outer Space: an Experience in Contemporary Law-Making, Sijthoff, Leiden, 1972.
[60] International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, United Nations General Assembly Resolution 56/83, 2001 approved by the.
[61] United Nations Group of Governmental Experts (UN GGE), Report of the group of governmental experts on developments in the field of information and telecommunications in the context of international security report, UN Doc A/70/174, in: M.N. Schmitt (Ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, second ed., Cambridge University Press, Cambridge, 22 July 2015, 2017. See also, e.g., Japan's Position Paper for the Report of the United Nations Open-Ended Working Group on "Developments in the Field of Information and Telecommunications in the Context of International Security" (undated) ('Japan recognizes that basic rules on State responsibility including those on countermeasures applies to cyberspace.'); Dutch Ministry of Foreign Affairs, Letter to the parliament on the international legal order in cyberspace (5 July 2019) ('Any violation of [obligations under international law that apply to states in cyberspace] that is attributable to a state constitutes an internationally wrongful act, unless there is a ground for precluding the wrongfulness of an act recognized in international law'); United Kingdom, Statement on Other Disarmament Measures and International Security to the 72nd UNGA First Committee (23 October 2017) ('We reaffirm that the law of state responsibility applies to cyber operations in peacetime').
[62] Article 2, Draft Articles on Responsibility of States for Internationally Wrongful Acts.
[63] Articles 20–26, Draft Articles on Responsibility of States for Internationally Wrongful Acts.
[64] Articles 28, 30 and 31, Draft Articles on Responsibility of States for Internationally Wrongful Acts.
[65] United Nations Office for Outer Space Affairs (UNOOSA), Guidelines for the Long-term Sustainability of Outer Space Activities of the Committee on the Peaceful Uses of Outer Space, UN Doc A/AC105/2018. https://www.unoosa.org/documents/pdf/PromotingSpaceSustainability/Publication_Final_English_June2021.pdf.
[66] United Nations Office for Outer Space Affairs (UNOOSA), Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space, UN Doc A/AC.105/890. https://www.unoosa.org/pdf/publications/st_space_49E.pdf.
[67] M.N. Schmitt (Ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, second ed., Cambridge University Press, Cambridge, 2017 https://doi.org/10.1017/9781316822524.
[68] Information technology — artificial intelligence — management system. ISO/IEC JTC 1/SC 42, ISO/IEC DIS 42001.
[69] IEEE Standard for Transparency of Autonomous Systems, VT/ITS – Intelligent Transportation Systems, IEEE, Mar. 2022, 7001-2021.
[70] United Nations Educational, Scientific and Cultural Organization (UNESCO), Recommendation on the ethics of artificial intelligence. https://unesdoc.unesco.org/ark:/48223/pf0000381137, 2021.
[71] United nations system Chief Executives board for coordination, principles for the ethical use of artificial intelligence in the United Nations system. https://unsceb.org/principles-ethical-use-artificial-intelligence-united-nations-system, 2022.
[72] Organisation for Economic Co-operation and Development (OECD), Recommendation of the Council on artificial intelligence, OECD/LEGAL/0449. https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449, 2019.
[73] World Economic Forum, Unpacking AI Procurement in a Box: Insights from Implementation, White Paper, 2022, in: https://www.weforum.org/publications/unpacking-ai-procurement-in-a-box-insights-from-implementation/.
[74] Under the doctrine of state responsibility, states are responsible for "wrongful" acts that are attributable to the state and breaches of an international obligation, Int'l Law Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries, Art. 2, Rep. of the Int'l Law Comm'n on the Work of Its Fifty-Third Session (2001). U.N. Doc. A/56/io.
[75] B.A. Koch, Liability for emerging digital technologies: an overview, J. Eur. Tort Law 11 (2) (2020) 115–136, https://doi.org/10.1515/jetl-2020-0137.
[76] P. Elson, Plane talking – a specialist risk publication for the aviation sector, Gallagher Specialty Q3 (2022) 1–28. Available at: https://www.ajg.com/uk/news-and-insights/2022/october/plane-talking-oct-2022/.
[77] H. Bang, Daphne: an intelligent assistant for architecting earth observing satellite systems, AIAA 2018-1366. 2018 AIAA Information Systems-AIAA Infotech @ Aerospace, Kissimmee, United States, 2018, pp. 8–12, https://doi.org/10.2514/6.2018-1366. January.
[78] R. Schmelzer, How is AI helping to commercialize space?. https://www.forbes.com/sites/cognitiveworld/2020/03/21/how-is-ai-helping-to-commercialize-space/, 21 March 2020 accessed 20.09.24.
[79] V. Shah, Next-generation space exploration: AI-enhanced autonomous navigation systems, Journal of Environmental Sciences and Technology (JEST) 3 (1) (2024) 47–68. https://jest.com.pk/index.php/jest/article/view/73.
[80] NASA's Scientific Visualization Studio, Tour of the Moon, 4K, 9 April 2018. https://science.nasa.gov/resource/tour-of-the-moon-4k/. accessed 20.09.24.
[81] A. Husain, The military applications of artificial intelligence in space. https://www.forbes.com/sites/amirhusain/2024/08/19/the-military-applications-of-artificial-intelligence-in-space/, 19 August 2024 accessed 20.09.24.
[82] N. Gable, BAE Systems to develop autonomous space-based surveillance technology. https://www.baesystems.com/en-us/article/bae-systems-to-develop-autonomous-space-based-surveillance-technology, 25 May 2023 accessed 20.09.24.
[83] S. Erwin, AI company developing software to detect hypersonic missiles from space. https://spacenews.com/ai-company-developing-software-to-detect-hypersonic-missiles-from-space/, 2024 accessed 20.09.24.
[84] S. Erwin, Slingshot unveils AI that spots satellite anomalies and potential bad actors. https://spacenews.com/slingshot-unveils-ai-that-spots-satellite-anomalies-and-potential-bad-actors/, 5 June 2024 accessed 20.09.24.
[85] J. Luckenbaugh, Lockheed Martin launches CJADC2 demo satellites. https://www.nationaldefensemagazine.org/articles/2024/5/6/lockheed-martin-launches-cjadc2-demo-satellites, 5 June 2024 accessed 20.09.24.
[86] Guiding principles, para. (a).
[87] Guiding principles, para. (b), (c), (d).
[88] Guiding principles, para. (d), (e).
[89] Wassenaar arrangement on export controls for conventional arms & dual-use goods & techs, Public Documents Volume I, Founding Documents, Dec. 2019. https://www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-I-Founding-Documents.pdf.
[90] Section V(1) and (2), Wassenaar Arrangement. Dual-use goods and technologies are listed in 9 categories with a 'sensitive' and 'very sensitive' list in the additional volume of the arrangement. According to the Arrangement, specific items are controlled within those categories of (1) special materials and related equipment, (2) materials processing, (3) electronics, (4) computers, (5) telecommunications, (6) sensors and lasers, (7) navigation and avionics, (8) marine, and (9) aerospace and propulsion Wassenaar arrangement on export controls for conventional arms & dual-use goods & techs, Public Documents Volume II, List of Dual-Use Goods and Technologies and Munitions List (2023), https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf.
[91] Section V(3) and (4), Wassenaar Arrangement.
[92] Section 7.D.2, Wassenaar List of Dual-Use Goods.
[93] Section 7.D.3.b, Wassenaar List of Dual-Use Goods.
[94] Z. Stanley-Lockman, E.H. Christie, An artificial intelligence strategy for NATO. https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html, 25 October 2021 accessed 20.09.24.
[95] High-level Expert Group on Artificial Intelligence (AI HLEG), Ethics guidelines for trustworthy AI. https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai, 8 April 2019 accessed 20.09.24.
[96] Council of Europe framework convention on artificial intelligence and human rights, democracy and the rule of law, Council of Europe Treaty (2024). Series – No. 225 (CETS 225), Vilnius, 5.IX, https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence.
[97] The fundamental principles of the Convention are: (a) human dignity and individual autonomy, (b) equality and non-discrimination, (c) respect for privacy and personal data protection, (d) transparency and oversight, (e) accountability and responsibility, (f) reliability, and (g) safe innovation.
[98] Article 3(2)-(4), Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.
[99] Article 3(2)-(3), Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.
[100] Article I(c), Liability Convention, 1972.
[101] In this sense, Graham and Thangavel further suggest clarification of the presented ambiguous terms within the OST and the LIAB, as well as possible adoption of 'presumption of causation' to ensure accountability on AI-driven or AI-supported launches, in: T. Graham, K. Thangavel (Eds.), Artificial Intelligence in Space: an Analysis of Responsible AI Principles for the Space Domain, IAC-23, E7,1,8, x77152, 74th International Astronautical Congress (IAC), Baku, Azerbaijan, 2023, pp. 2–6. October.
[102] R.F. Trager, L.M. Luca, Killer robots are here – and we need to regulate them. https://foreignpolicy.com/2022/05/11/killer-robots-lethal-autonomous-weapons-systems-ukraine-libya-regulation/, 2022 accessed 20.09.24.
[103] Z. Kallenborn, Applying arms-control frameworks to autonomous weapons. https://www.brookings.edu/articles/applying-arms-control-frameworks-to-autonomous-weapons/, 5 October 2021 accessed 20.09.24.
[104] M. Taddeo, A. Blanchard, Accepting moral responsibility for the actions of autonomous weapons systems – a moral gambit, Philos. Technol. 35 (2022) 1–24, https://doi.org/10.1007/s13347-022-00571-x.
[105] V. Boulanin, M. Bo, Three lessons on the regulation of autonomous weapons systems to ensure accountability for violations of IHL. https://blogs.icrc.org/law-and-policy/2023/03/02/three-lessons-autonomous-weapons-systems-ihl/, 2 March 2023 accessed 20.09.24.
[106] World Intellectual Property Organization (WIPO), What is Intellectual Property? Undated, https://www.wipo.int/about-ip/en/(accessed 20.09.24).
[107] "A patent is an exclusive right granted for an invention, which is a product or a process that provides, in general, a new way of doing something, or offers a new

technical solution to a problem." See WIPO, Patents, undated, https://www.wipo.int/web/patents (accessed 20.09.24).
[108] Copyright (or author's right) is a legal term used to describe the rights that creators have over their literary and artistic works. Works covered by copyright range from books, music, paintings, sculpture, and films, to computer programs, databases, advertisements, maps, and technical drawings." See WIPO, Frequently Asked Questions: Copyright, undated, https://www.wipo.int/copyright/en/faq-copyright.html (accessed 20.09.24).
[109] A trademark is a sign capable of distinguishing the goods or services of one enterprise from those of other enterprises." See WIPO, Trademarks, undated, https://www.wipo.int/trademarks/en/(accessed 20.09.24).
[110] "In a legal sense, an industrial design constitutes the ornamental aspect of an article." See WIPO, Industrial Designs, undated, https://www.wipo.int/designs/en/(accessed 20.09.24).
[111] A geographical indication (GI) is a sign used on products that have a specific geographical origin and possess qualities or a reputation that are due to that origin." See WIPO, Geographical Indications, undated, https://www.wipo.int/geo_indications/en/(accessed 20.09.24).
[112] Trade secrets are intellectual property (IP) rights on confidential information which may be sold or licensed." See WIPO, Trade Secrets, undated, https://www.wipo.int/tradesecrets/en/(accessed 20.09.24).
[113] Article 3(33), Artificial Intelligence Act.
[114] D.A. Zetoony, Understanding AI terms: what is input data?. https://www.gtlaw-dataprivacydish.com/2023/08/understanding-ai-terms-what-is-input-data/, 2023 accessed 20.09.24.
[115] Should the status quo change and machine learning become a reality in space, a legal question will inevitably arise regarding the IP protection for data sets utilized in this context. See unauthored, Researchers successfully train a machine learning model in outer space for the first time. https://www.ox.ac.uk/news/2023-07-28-researchers-successfully-train-machine-learning-model-outer-space-first-time, 28 July 2023 accessed 20.09.24.
[116] J. Walsh, How to identify key intellectual property in Machine Learning projects, undated, https://gemmo.ai/intellectual-property-protection-for-ai/(accessed 20.09.24).
[117] J. Saltz, What is the AI life cycle?. https://www.datascience-pm.com/ai-lifecycle/, 31 March 2024 accessed 20.09.24.
[118] C3 AI, Model Training, undated, https://c3.ai/glossary/data-science/model-training/(accessed 20.09.24).
[119] Unauthored, Exploitation and exploration in machine learning. https://www.geeksforgeeks.org/exploitation-and-exploration-in-machine-learning/, 2024 accessed 20.09.24.
[120] A. Gulati, Artificial intelligence life cycle: from conception to production. https://www.knowledgehut.com/blog/data-science/artificial-intelligence-life-cycle, 29 December 2023 accessed 20.09.24.
[121] D. Coleman, Legal principles around copyright on data used for AI training. https://www.linkedin.com/pulse/legal-principles-around-copyright-data-used-ai-training-david-coleman-yqvpc, 2024 accessed 20.09.24.
[122] J. Quang, Does training AI violate copyright law? Berk. Technol. Law J. 36 (2021) 1408–1436. https://btlj.org/wp-content/uploads/2023/02/0003-36-4Quang.pdf.
[123] NASA Earthdata, Your Gateway to NASA Earth Observation Data, undated, https://www.earthdata.nasa.gov (accessed 20.09.24).
[124] ITU News, How AI can unlock space data to improve lives, faster. https://www.itu.int/hub/2020/03/how-ai-can-unlock-space-data-to-improve-lives-faster/, 26 March 2020 accessed 20.09.24.
[125] U.S. Unauthored, Copyright Office fair use index. https://www.copyright.gov/fair-use/, November 2023 accessed 20.09.24.
[126] J.R. Butler, How licensing models can Be used for AI training data. https://variety.com/vip/why-generative-ai-companies-will-pay-content-owners-and-licensing-models-that-will-emerge-1235944577/, 19 March 2024 accessed 20.09.24.
[127] Unauthored, Data scraping or mining copyright protected works, undated, https://www.copyrightuser.org/understand/data-scraping-data-mining-copyright-protected-works/(accessed 20.09.24).
[128] S. Jain, A. Agrawal, AI and copyright: legal perspectives on transformative and extractive uses of copyrighted works. https://www.medianama.com/2024/07/223-ai-copyright-legal-perspectives-transformative-extractive-uses-copyrighted-works/, 2 July 2024 accessed 20.09.24.
[129] D.A. Garay, Powering artificial intelligence with data: why quality matters. https://www.linkedin.com/pulse/powering-artificial-intelligence-data-why-quality-daniel-abate-garay-7llye, 28 February 2024 accessed 20.09.24.
[130] IBM, What is an AI model? Undated, https://www.ibm.com/topics/ai-model (accessed 20.09.24).
[131] AI Collective, Output of AI Algorithms, undated, https://www.aicollective.co/output-of-ai-algorithms (accessed 20.09.24).
[132] National Environmental Satellite, Data, and information service (NOAA), transforming energy into imagery: how satellite data becomes stunning views of earth. https://www.nesdis.noaa.gov/news/transforming-energy-imagery-how-satellite-data-becomes-stunning-views-of-earth, 2020 accessed 20.09.24.
[133] ESA, Industry and, Intellectual property. https://www.esa.int/About_Us/Business_with_ESA/How_to_do/ESA_Industry_and_Intellectual_Property, 19 November 2014 accessed 20.09.24.
[134] Unauthored, Understanding how Satellite Images are created. https://skywatch.com/understanding-how-satellite-images-are-created/, 28 April 2022 accessed 20.09.24.
[135] M. Adhikari, Legal Regime of Intellectual Property Rights of Spatial Data with Special Reference to India, Geospatial World Forum, Hyderabad, India, 2011, 18 – 21 January, https://geospatialworldforum.org/2011/proceeding/pdf/Malay%20AdhikarifullPaper.pdf.
[136] In contrast to the United States, the European Union is more amenable to the concept of copyrighting AI outputs. However, the EU's stance is contingent upon the necessity of a "significant form of human input." Moreover, the interpretation of the Court of Justice of the European Union's (CJEU) ruling remains at the discretion of each member state, The United Kingdom's position aligns with that of the EU, yet it may be more receptive to the notion of copyright protection for generative AI outputs, a standpoint that China also appears to espouse. See unauthored, Copyright Ownership of Generative AI Outputs Varies Around the World (29 January 2024). https://www.cooley.com/news/insight/2024/2024-01-29-copyright-ownership-of-generative-ai-outputs-varies-around-the-world. accessed 20.09.24.
[137] https://www.copyrightuser.org/create/writer/(accessed 20.09.24).
[138] Unauthored, Introduction to International Copyright Law, 7 February 2023, https://www.copyrightlaws.com/introduction-international-copyright-law/(accessed 20.09.24).
[139] Unauthored, 8. Do I have copyright in my work in other countries? Undated, https://www.copyrightuser.org/faqs/question-8/(accessed 20.09.24).
[140] WIPO, Copyright, undated, https://www.wipo.int/copyright/en/(accessed 20.09.24).
[141] P. Gangmeih, The relationship between outer space activities and intellectual property laws, educational administration, Theory and Practice 30 (1) (2024) 741–748.
[142] C.W. Lackert, IP in outer space: the next frontier. https://www.inta.org/perspectives/features/ip-in-outer-space-the-next-frontier, 8 December 2021 accessed 20.09.24.
[143] S. Ayalp, Lost in space: the copyright dilemma, Intellectual Property Brief 7 (2) (2020) 86–112. https://digitalcommons.wcl.american.edu/ipbrief/vol7/iss2/1.
[144] B. Fung, Only real people can patent inventions – not AI – US government says. https://edition.cnn.com/2024/02/14/tech/billions-in-ai-patents-get-new-regulations/index.html, 2024 accessed 20.09.24.
[145] E.D. Lanquist, D. Rota, Intellectual property legal issues impacting artificial intelligence. https://www.bakerdonelson.com/intellectual-property-legal-issues-impacting-artificial-intelligence, 2023 accessed 20.09.24.
[146] I.I. Article, Outer Space Treaty, 1967.
[147] A. Blijlevens, Intellectual property protection for satellites and outer space technologies. https://www.ajpark.com/insights/intellectual-property-protection-for-satellites-and-outer-space-technologies/, 20 June 2018 accessed 20.09.24.
[148] Y. Zhao, Intellectual property protection in outer space: reconciling territoriality of intellectual property with non-territoriality in outer space, Queen Mary J. Intell. Prop. 7 (2) (2017) 137–155, https://doi.org/10.4337/qmjip.2017.02.01.
[149] R. Oosterlinck, The intergovernmental space station agreement and intellectual property rights, J. Space Law 17 (1) (1989) 23–36.