www.gfprjournal.com
GFPR
GLOBAL FOREIGN POLICIES REVIEW

p-ISSN: 2788-502X
e-ISSN: 2788-5038

GFPR

GLOBAL FOREIGN POLICIES REVIEW

HEC-RECOGNIZED CARTEGORY-Y

DOI (Journal): 10.31703/gfpr
DOI (Volume): 10.31703/gfpr/.2025(VIII)
DOI (Volume): 10.31703/gfpr/.2025(VIII.III)

VOL. VIII, ISSUE III, SUMMER (SEPTEMBER-2025)

Double-blind Peer-review Research Journal
www.gfprjournal.com

HumanityPublications
sharing research

Humanity Publications(HumaPub)
www.humapub.com
Doi: https://dx.doi.org/10.31703

Article Title

National Security, Artificial Intelligence, and Sovereignty beyond Earth: Reconstructing the Legal Architecture of Space Intelligence Networks

Abstract

Artificial intelligence (AI) is now a determining factor in the development of outer-space operations. The national security, intelligence, and early warning systems are currently under the influence of autonomous satellites, constellations of sensors, and deep-learning algorithms. However, the existing legal framework, which is based on the Outer Space Treaty of 1967, is insufficient to support the transparency and autonomy of AI. The article analyzes the challenges of sovereignty and accountability faced by states due to algorithmic decision-making. It reclaims the legal framework of space intelligence networks by proposing a stratified structure of sovereignty, along with physical, algorithmic, and institutional novelty, such as a Space Intelligence Authority. Based on comparative space law, AI governance theory, and normative fairness analysis, this paper proposes a design of a regulatory framework for space-based intelligence that not only pertains to the control of the territory but also addresses the algorithmic and AI-based decision-making in space.

Keywords: Artificial Intelligence, National Security, Space law, Sovereignty, Accountability, liability, Outer Space Treaty, AI governance

Authors:

Bakht Munir: (Corresponding Author)
Postdoctoral Fellow, The University of Kansas School of Law, USA.
(Email: bakht.munir@ku.edu)

Ali Nawaz Khan: Assistant Professor, University Law College, University of the Punjab, Lahore, Punjab, Pakistan.

Muhammad Arslan: LLM Scholar, Pennsylvania State University, USA.

Pages: 29-37
DOI: 10.31703/gfpr.2025(VIII-III).04
DOI link: https://dx.doi.org/10.31703/gfpr.2025(VIII-III).04
Article link: https://gfprjournal.com/article/national-security-artificial-intelligence-and-sovereignty-beyond-earth-reconstructing-the-legal-architecture-of-space-intelligence-networks
Full-text Link: https://gfprjournal.com/article/national-security-artificial-intelligence-and-sovereignty-beyond-earth-reconstructing-the-legal-architecture-of-space-intelligence-networks
Pdf link: https://www.gfprjournal.com/jadmin/Auther/31rvIolA2.pdf

Global Foreign Policies Review

p-ISSN: 2788-502X **e-ISSN:** 2788-5038
DOI(journal):10.31703/gfpr
Volume: VIII (2025)
DOI (volume):10.31703/gfpr.2025(VIII)
Issue: III Summer (September-2025)
DOI(Issue): 10.31703/gfpr.2025(VIII-III)

Home Page
www.gfprjournal.com

Volume: VIII (2025)
https://www.gfprjournal.com/Current-issue

Issue: III-Summer (September-2025)
https://www.gfprjournal.com/issue/8/3/2025

Scope
https://www.gfprjournal.com/about-us/scope

Submission
https://humaglobe.com/index.php/gfpr/submissions

Visit Us

Humanity Publications (HumaPub)
www.humapub.com
Doi: https://dx.doi.org/10.31703

Citing this Article

04	National Security, Artificial Intelligence, and Sovereignty beyond Earth: Reconstructing the Legal Architecture of Space Intelligence Networks		
Authors	Bakht Munir Ali Nawaz Khan Muhammad Arslan	DOI	10.31703/gfpr.2025(VIII-III).04
		Pages	29-37
		Year	2025
		Volume	VIII
		Issue	III

Referencing & Citing Styles

APA	Munir, B., Khan, A. N., & Arslan, M. (2025). National Security, Artificial Intelligence, and Sovereignty beyond Earth: Reconstructing the Legal Architecture of Space Intelligence Networks. *Global Foreign Policies Review*, *VIII*(III), 29-37. https://doi.org/10.31703/gfpr.2025(VIII-III).04
CHICAGO	Munir, Bakht, Ali Nawaz Khan, and Muhammad Arslan. 2025. "National Security, Artificial Intelligence, and Sovereignty beyond Earth: Reconstructing the Legal Architecture of Space Intelligence Networks." *Global Foreign Policies Review* VIII (III):29-37. doi: 10.31703/gfpr.2025(VIII-III).04.
HARVARD	MUNIR, B., KHAN, A. N. & ARSLAN, M. 2025. National Security, Artificial Intelligence, and Sovereignty beyond Earth: Reconstructing the Legal Architecture of Space Intelligence Networks. *Global Foreign Policies Review,* VIII**,** 29-37.
MHRA	Munir, Bakht, Ali Nawaz Khan, and Muhammad Arslan. 2025. 'National Security, Artificial Intelligence, and Sovereignty beyond Earth: Reconstructing the Legal Architecture of Space Intelligence Networks', *Global Foreign Policies Review*, VIII: 29-37.
MLA	Munir, Bakht, Ali Nawaz Khan, and Muhammad Arslan. "National Security, Artificial Intelligence, and Sovereignty Beyond Earth: Reconstructing the Legal Architecture of Space Intelligence Networks." *Global Foreign Policies Review* VIII.III (2025): 29-37. Print.
OXFORD	Munir, Bakht, Khan, Ali Nawaz, and Arslan, Muhammad (2025), 'National Security, Artificial Intelligence, and Sovereignty beyond Earth: Reconstructing the Legal Architecture of Space Intelligence Networks', *Global Foreign Policies Review,* VIII (III), 29-37.
TURABIAN	Munir, Bakht, Ali Nawaz Khan, and Muhammad Arslan. "National Security, Artificial Intelligence, and Sovereignty Beyond Earth: Reconstructing the Legal Architecture of Space Intelligence Networks." *Global Foreign Policies Review* VIII, no. III (2025): 29-37. https://dx.doi.org/10.31703/gfpr.2025(VIII-III).04.

e-ISSN: 2788-5038 Volume: VIII (2025) Issue: III-Summer (September-2025) p-ISSN: 2788-502x

Global Foreign Policies Review
www.gfprjournal.com
DOI: http://dx.doi.org/10.31703/gfpr

Pages: 29-37 URL: https://doi.org/10.31703/gfpr.2025(VIII-III).04 Doi: 10.31703/gfpr.2025(VIII-III).04

Cite Us

Title

National Security, Artificial Intelligence, and Sovereignty beyond Earth: Reconstructing the Legal Architecture of Space Intelligence Networks

Authors:

Bakht Munir: (Corresponding Author)
Postdoctoral Fellow, The University of Kansas School of Law, USA.
(Email: bakht.munir@ku.edu)

Ali Nawaz Khan: Assistant Professor, University Law College, University of the Punjab, Lahore, Punjab, Pakistan.

Muhammad Arslan: LLM Scholar, Pennsylvania State University, USA.

Abstract

Artificial intelligence (AI) is now a determining factor in the development of outer-space operations. The national security, intelligence and early warning systems are currently under the influence of autonomous satellites, constellations of sensors, and deep-learning algorithms. However, the existing legal framework, which is based on the Outer Space Treaty of 1967, is insufficient to support the transparency and autonomy of AI. The article analyzes the challenges of sovereignty and accountability faced by states due to algorithmic decision-making. It reclaims the legal framework of space intelligence networks by proposing a stratified structure of sovereignty, along with physical, algorithmic, and institutional novelty, such as a Space Intelligence Authority. Based on comparative space law, AI governance theory, and normative fairness analysis, this paper proposes a design of a regulatory framework for space-based intelligence that not only pertains to the control of the territory but also addresses the algorithmic and AI-based decision-making in space.

Keywords:

Artificial Intelligence, National Security, Space Law, Sovereignty, Accountability, Liability, Outer Space Treaty, AI Governance

Contents

Introduction

The twenty-first century has changed outer space from being an exploration frontier to a strategic contestation sphere. The ongoing militarization and commercialization of orbital operations have erased the distinction formerly existing between geopolitical conquest and scientific discovery. Modern nations wouldn't be able to maintain their national security without satellites, as they are the technological foundation of communications, reconnaissance, navigation, and early-warning systems (Wark, 2025). As artificial intelligence (AI) becomes more and more intertwined with both orbital and ground-station operations, states have started to rely more on

autonomous programs to categorize threats, interpret sensor data, and coordinate defensive actions with minimum human involvement (Tricco, 2025).

This technological change upsets the normative basis of the international space law. The classical regime forming the base for the Outer Space Treaty of 1967 was designed in a time when the possibility of subjecting machines to surveillance and controlling them existed. Its terms on state responsibility and peaceful use require that machines are under full control of humans (Abashidze et al., 2022; Pagallo, 2023; Munir, 2025). The modern AI systems, on the contrary, develop as a result of autonomous learning cycles, producing decisions that even their creators cannot foresee (Li, 2025; Abbasi, et. al., 2025). This sort of autonomy disintegrates the historical chain of command and creates what researchers refer to as an accountability gap wherein the legal accountability cannot be effortlessly identified (Burri, 2017). The issue doesn't only exist in the sphere of space but also in the domain of state authority. Human control over autonomous satellites is retrospective, as their actions are executed in milliseconds, often preemptively, without real-time human intervention. According to Raza (2024), instead of adding fairness and transparency as the external protection, they need to be part of the algorithm design (Munir et. al., 2025). These implications, when applied to space operations, are that the legal responsibility has to emerge out of the inherent auditability and co-governance systems that can track algorithmic logic.

In this regard, the development of AI-driven space systems requires a redesigned legal framework, one that rides on collaboration but keeps up with autonomy. The law and policy issue is that as intelligence in orbit becomes more autonomous, it must be beholden to the values of responsibility, equity, and collective security as opposed to the secrecy of code.

The Role of Space Intelligence in AI

The combination of artificial intelligence and orbital technologies is one of the most significant changes in the contemporary architecture of national security. The space-intelligence networks have transformed into distributed ecosystems that combine orbital sensors, land receivers, and sophisticated machine-learning structures with the ability to process large amounts of data in real time (CSET, 2025). Human-directed surveillance is being usurped by intelligent automation very quickly, where deep-learning algorithms outline any anomalies, label debris, and predict possible hostilities between orbital layers (Hu et al., 2025). These neural architectures process sensor inputs with incredible speed and detect small changes in radiation, motion, or communication frequencies that need not be noticed by human analysts. Consequently, AI is becoming the heart of missile-defense coordination, satellite navigation, and high-latency communications with instant interpretative decision-making (European Space Agency, 2018).

Outside the efficiency in operations, the engagements of AI redefine the logics of command authority. Orbit-recalibration and encryption algorithms, as well as autonomous re-allocation of bandwidth, introduce a quasi-actor into a security chain, a legal personality-free entity but one that can change the outcome of a strategic decision (Chesterman, 2020). There is an increasing independence of these systems, which reduces the previous distinctiveness between decision-makers and instruments. Researchers refer to this as delegated intent, whereby some of the human discretion is transferred into algorithms (Lin, 2012). The role of the human would be more retrospective when an AI system is changing the posture of satellites or making a collision-avoiding maneuver in milliseconds. Post-hoc assessments can be used to detect anomalies in the processes; however, rarely do they reinstitute the human agency dispossessed in such critical moments of machine rule. Within this framework, accountability will be redefined not as individual responsibility but as a virtual management of error in calculation.

Such a change places AI-powered space networks at the crossroads of science and technology, legislation, and geopolitics. Machine inference velocity shrinks the temporal constraints on decision-making; the process of strategic deliberation passes out of human deliberation and is a pre-programmed parameter. As such, the issue isn't confined to engineering but rather to the validity of autonomous rule in areas that invoke sovereignty, security, and peace.

Weaknesses of the Current Legal System:

The Outer Space Treaty and Crisis of Responsibility

The principles of the international laws of space formulated in the 1967 Outer Space Treaty (OST) reflected an age of human domination and controlled mechanical functioning. In Article VI, it's envisaged that the states have international accountability regarding the activities that are undertaken in outer space, even those that are undertaken by the private or non-state players operating under their jurisdiction (Kopal, 1966). This expression assumes that the government can impose effective control on all the entities that work on its behalf. The fact that autonomous systems are coming up will essentially break this assumption as control gets diluted and ex post, as opposed to continuous, when algorithms independently decide the moves of satellites or decode intelligence data (Li, 2025).

The resulting fault gap represents the legal inertia between human will and algorithmic actions and the impossibility of identifying possible liability when

autonomous actions aren't based on design specifications (Bratu et al., 2021). The classical theories of negligence or intent cannot explain this ambiguity, which in turn demeans deterrence and reparations. Practically, states can deny direct fault when the victims won't even be compensated. The disconnect increases because machine learning systems are self-optimizing in nature and regularly yield results for which no programmer would be explicit about the result. The language of the OST of authorization and continuing supervision, which in this manner, therefore, seems to be progressively of less control with intelligent systems that cannot be controlled continuously.

Convention and Algorithmic Causation of Liability

The Liability Convention of 1972 expounded this concept of compensation by drawing the line between an absolute liability in surface damage and a litigable liability in space accidents (Hobe et al., 2013). The dichotomy presupposes a chain of causation—an act or omission that can be traced back to a person or organ of responsibility. AI negates such an assumption. Machine-learning systems are developed by undergoing non-deterministic training loops, which result in actions that the creators of the machine-learning system can hardly explain (Bayern, 2015). This makes foreseeability, which forms a part of the doctrine of liability, become indeterminate.

Was it a fault in the architecture of the autonomous satellite, its training data, or the failure of the supervising state to restrict autonomy that led to an autonomous satellite, acting on adaptive reinforcement algorithms, hitting another spacecraft after recalculation of an orbital path? (Li, 2025). None of these groups can fit well into the binary logic of the Convention. Strict liability would be unfair in the case of states that were acting in due diligence; fault-based liability will fail in case fault is an emerging property of algorithmic design. The lack of explicit attribution systems makes the existing regime inappropriate in a world where it isn't operators but algorithms that define the movement and danger in space.

Non-appropriation and Data Authority

This procedure entails recognizing that data is continuously changing all around us (Gupta et al., 2014). Non-Appropriation and Data Authority: This process involves acknowledging the fact that the data is continuously transforming everywhere around us (Gupta et al., 2014).

The OST non-appropriation provision, which found its reflection in the 1979 Moon Treaty, doesn't allow the exercise of sovereignty over the celestial territory (Moon Treaty, 1979). However, this spatial limitation isn't maintained in informational or digital space. The manipulation of information in the era of AI serves as a surrogate for the manipulation of space. Satellite constellations are constantly reaping off high-resolution imagery, spectral signatures, and telemetry information, the strategic utility of which is much greater than that of physical occupation. Nevertheless, none of the treaties describe the ownership or sharing of such datasets (Hu, 2024).

Another trend setting a new power dynamic in space governance is data sovereignty, which particularizes the control over the process of information gathering, data storage, and processing (Manheim and Kaplan, 2019). Monopolization of access to orbital information by states is an effective way of establishing the international intelligence order. The concept of common heritage will become a disjointed system of proprietary monopolies without mutually accepted standards of data exchange or privacy protection (Carrillo, 2020; Raza, et. al., 2024). The absence of the law allows technologically superior countries to concentrate power in their hands in the name of commercial secrecy at the expense of the developing countries and to undermine the spirit of cooperation that was envisaged by the initial space law.

Audit Deficiency and Lack of Transparency

The OST (as well as its successor conventions) doesn't impose the concepts of algorithmic transparency, explainability, or auditing. Checking is based mostly on state statements and not on empirical examination (Council of Europe, 2019). The latest examples of soft-law proposals, such as the Recommendation on the Ethics of Artificial Intelligence by UNESCO or self-regulation by the industry, are encouraging responsible AI but don't force it (Soroka and Kurkova, 2019). Absent a binding standard, national security interests tend to support the use of secrecy, which wouldn't subject AI activities to international investigation.

Such institutional shortcomings create suspicion and strategic instability. In the scenario where the states are unable to determine the dependability or maliciousness of autonomous systems, each orbital maneuver can be construed as aggression. The lack of compulsory audit systems not only undermines accountability but also hinders crisis management. According to Novelli et al. (2024), algorithmic systems must be tested and certified on a regular basis so that they align with the normative expectations; however, these processes are new to space law. The technological independence of legal accountability, therefore, forms one of the greatest emergent issues of the new space order.

Rebuilding the Legal Architecture:

Foundational Norms

To recreate the legal governance of AI in space, it's crucial to place it within a consistent framework of principles that would contain both technological facts and non-negotiable values.

- The first is functional sovereignty, which doesn't place power in the possession of a territory but in the management and control of operations and the stewardship (Pagallo, 2023). This vision identifies sovereignty with the duties of the control of algorithmic and data infrastructures as opposed to the ownership of heavenly land.
- Second is the auditing, which entails the fact that AI pathways to decisions must be capable of being traced and verified by standardized logs and transparency frameworks (Novelli et al., 2024). Responsibility falls apart when there is no trace.
- Third, human control should also be maintained. Rationalized systems can speed up efficiency, but cannot substitute normative judgment. Human-in-the-loop mechanisms should be maintained in strategic operations involving possible conflict or intelligence exploitation to create moral and legal responsibility (Lin, 2012).
- Fourth, to avoid normative fragmentation, interoperability is necessary. Standard legal and technical conventions facilitate the data interchange, minimize the lack of understanding, and establish trust between the spacefaring entities (European Space Agency, 2018).
- Last but not least, equity requires the developing states to be meaningfully accessed by technological and institutional resources. According to Raza (2024), fairness in the systems of artificial intelligence needs to be systemic, which means that innovation shouldn't support inequality. In the case of outer space, equity is used to make sure that the influence on AI governance isn't restricted to technologically superior powers.

Layered Sovereignty Model

It is based on these pillars that a three-pillar model separates physical, data, and algorithmic sovereignty.

- Physical sovereignty involves concrete infrastructure—satellites, launch vehicles, and ground control centers—and is consistent with current rules of registration and liability (Kopal, 1966).
- Data sovereignty is the extension of authority over information produced with the help of such systems, employing it to control the data gathering, storing, and sharing (Hu, 2024). It brings in privacy commitments, the access procedures, as well as mutual data-sharing clauses to avoid monopolies.
- The next most recent layer is algorithmic sovereignty, which claims control over the design, deployment, and behavior of AI models *per se* (Pagallo, 2023). It involves management of training data, update schedules, and built-in ethical standards.

By isolating these domains, accountability is enabled to be assigned in a precise manner. A state could have an algorithmic control and control of data, whereas physical custody of satellites could be kept by a private contractor. This stratified system allows a combination of the work of the state and the business in ways that don't weaken state accountability (Alarie et al., 2016). It also establishes space for adaptive control, where various mechanisms of oversight are exercised on diverse levels of sovereignty.

Institutional Infrastructure

Layered sovereignty requires institutional innovation in order to be effective in practice. An AI-powered satellite may be registered through a Space Intelligence Authority (SIA) that would be led by the United Nations and certify adherence to algorithms, as well as investigate incidents (Abashidze et al., 2022). The SIA would also be a regulator and moderator, and it would enjoy the transparency, compliance, and audit requirements of the states. Domestic inspections would be carried out by Complementary National AI Audit Bureaus (NAABs), and algorithmic logs would be made available and coordinated for reporting to SIA (Novelli et al., 2024). This model of two levels balances between national autonomy and collective verification on the one hand and inspection frameworks applied in nuclear safety and environmental regimes on the other hand (National Security Commission on AI, 2021).

This type of arrangement encourages confidence amongst each other and eliminates duplication. States would maintain sovereignty but provide technical data to be verified by multilateral bodies, which would enhance the validity of AI activity. In the long term, standardized audit practices would result in the establishment of a best practice bank that can be used by both the military and the civilian worlds.

Modular Treaty Design

Considering the fast pace of development of AI technology, treaty rigidity poses the risk of obsolescence. The development of AI Regime Protocols (modular annexes revised on a regular basis to incorporate new standards) should be applied in the future when it comes to governance (Pagallo, 2023). These annexes would create certification measures, reporting, and liability systems through verified audit evidence (Li, 2025).

Modularity ensures continuity in addition to responsiveness in that amendments can be made without necessarily reopening core treaties. The efficiency of such adaptive instruments is proven by the historical precedent of the environmental agreements (Hobe et al., 2013).

Fairness and Ethical Oversight

An equitable and ethical regulation of the scientific field is expected, and the same case is likely to be observed in this case. Any legal system is legitimate based on its ability to balance innovation with justice. The introduction of fairness into the governance of AI in space corresponds to the claims made by Raza (2024) that the lack of transparency and equal access is the precondition to gaining the trust of the population. Fairness in space intelligence doesn't just stop at distributive equality but also encompasses procedural protection, which is that the decisions made by algorithms can be explained and reviewed (Carrillo, 2020). Through institutionalization of fairness, i.e., open audit systems, shared databanks, and nondiscriminatory licensing, space law transforms a reactive dispute-settlement apparatus into a proactive ethical administration regime. Through this, the lawfulness of outer space will be able to maintain technological dynamism and normative legitimacy. Fairness, therefore, isn't only an ideal but also a constituent of the structural transition of sovereignty and solidarity in the era of autonomous intelligence.

Policy Recommendations and pathways to implementation:

Phased Adoption

The application of a legal structure of AI-driven space intelligence into practice cannot be rendered suddenly. It has to be done in a highly gradual manner that acknowledges the imbalance in terms of technological capability, confidence, and geopolitical orientation.

- An initial coalition of advanced AI and orbital infrastructures should be implemented, consisting of the states and intergovernmental entities with the most developed AI and missions abducted under the provisional certification by the proposed Space Intelligence Authority (SIA) (CSET, 2025). Such early adopters would become the normative point of reference, showing that transparency, algorithmic auditability, and operational accountability can be consistent with national security goals.
- Pilot projects would be used to push the key compliance capabilities, including audit pipelines based on algorithms, transparency boards, and log-checking systems (Hu et al., 2025). These technical exercises would be done under the SIA supervision to prove the concept, as well as detect procedural vulnerabilities. They would also experiment on how audit mechanisms can operate without divulging classified or commercially sensitive information.
- The following stages ought to institutionalize capacity-building measures of the developing and emerging space actors. This inclusion is important not only to be fair but also to legitimize the regimes themselves. The value of common technological capability in multilateral governance isn't new to the European Space Agency (2018) and the like. Training programs, open audit tools, and model legal frameworks could be funded by a special SIA fund funded by membership fees and voluntary contributions to enable the developing countries to reach the compliance requirements. Subsidization of participation might also be provided by favoring access to data-sharing networks, collaborative satellites, and reduced audit certification.

This gradual development, by the movement of pilot coalitions to comprehensive growth, would be organic instead of forceful. The initial adopters would perfect the rules by trial and error, which would enable the later entrants to have a stable and proven regime. This cycle of development would, in the long term, transform a collection of experimental procedures into a powerful international rule system that can control AI-driven space intelligence with both discretion and power.

Verification and Enforcement

Checking and balancing are the working principles of any reputable legal system. In their absence, standards are going to degenerate into aspirational rhetoric. In the framework of space intelligence, verification should strike a balance between two conflicting demands: the necessity of openness and the secrecy of sensitive technological data. Secure audit trails and cryptographic verification systems achieve a functional equilibrium, that is, they are recording the behavior of algorithms without exposing the proprietary source code (Novelli et al., 2024).

Studded Cryptography Proofs: A cryptographic proof may allow outside auditors to verify algorithm compliance without being exposed to the algorithm. This method is similar to the data protection methods that are implemented in financial and cybersecurity audits (Irfan, et. al., 2024). It not only supports state sovereignty but also verifiability so that the independent checkers under the SIA can ensure the AI systems meet international standards, while they can retain the secrecy of the operation.

Enforcement, conversely, must be carried out by a mechanism of escalated incentives and punishments. States that comply with verification requirements might be offered preferential treatment, such as faster registration of orbital assets or due process of shared

frequencies, or be able to engage in cooperative intelligence sharing (National Security Commission on AI, 2021). On the other hand, repeated non-compliance may provoke similar sanctions: a temporary loss of registry recognition or surcharge of the liability in accordance with the amendments to the Liability Convention (Hobe et al., 2013).

Procedural fairness also determines the credibility of enforcement. The SIA should have an open and transparent system of appeals by which accused states or corporations can appeal. When making decisions, the basis should be verifiable audit records and not diplomacy. In the long run, the stable use of clear procedures will turn the enforcement into a partnership rather than coercive supervision, which will support the rule of law and mutual trust in the sphere of orbital space.

Technical and Political Implications

The technical and political resistance that the proposed architecture will face is going to be formidable despite its normative appeal. The most significant issue is the conflict of sovereignty and collective supervision. The defense systems are traditionally the prerogative of the sovereignty of national security establishments. The very idea of submitting such systems to external audit, even in part, triggers the internal fears of being a spy, vulnerable, and without strategic autonomy (Tricco, 2025).

The second technical obstacle is the existing infrastructure, which is the pre-integration of AI audit modules. Most of the current satellites do not have onboard data-logging systems or secure channels of communication that can be used to verify SIA protocols (Friedland & Lum, 1987). The cost of retrofitting these systems is very high and can lead to disruption of ongoing missions. The states can reduce these loads by implementing a transitional model that would emphasize new missions to achieve complete compliance and allow old assets some flexibility.

Graduated implementation can be used to ease diplomatic resistance. First audits may not even examine sensitive intelligence algorithms: instead, they may simply look at non-classified operational metrics, including the accuracy of telemetry, system availability, and performance of collision avoidance, etc. (Pagallo, 2023). With institutional trust developing, the scope of an audit might gradually increase to more extensive degrees of algorithmic transparency. Such a strategy reflects the development of verification standards in nuclear disarmament, in which intrusive inspections were developed only decades after confidence-building.

Besides, political buy-in relies on fair governance. The developing countries have to view the regime not as a means to technological domination but as a shared insurance in case of systemic risk against all space actors. It is therefore important to frame the SIA as a technocratic institution as opposed to a geopolitical consortium. In its governance, it should include equal representation in the regions, rotating leadership, and decision-making processes that are not influenced by veto politics.

TG Integration with Terrestrial AI Governance

An integrated international system cannot consider orbital regulation without including terrestrial AI regulation. The algorithms that are used in the orbit are frequently designed, trained, and tested in the domestic legal systems. The discrepancy between the Earth and the alien state may result in regulatory issues, openings, and unequal responsibility. An example is that an AI model that is certified by the national law may not comply with the standards of transparency in orbital deployment, leaving it unclear which standard is better than the other (Hu, 2024).

To prevent these contradictions, the principles of the primary terrestrial systems, including the AI Act of the European Union and the executive regulations of the United States on trustworthy AI, must be applied to the space operations (Novelli et al., 2024). The frameworks lay stress on transparency, proportional risk assessment, and human control, all of which can be applied to the orbital environment. Standard harmonization not only makes life easier when it comes to complying with multinational corporations but also enhances a cohesive international ethic of mindful AI (Manheim and Kaplan, 2019).

Global bodies such as the OECD and the Global Partnership on Artificial Intelligence of the G7 may act as intermediaries between the ruling of the earth and that of the aliens. They are capable of organizing cross-domain audits, delivering interpretive direction, and aligning data security standards. This type of integration can help to make AI that is sent into space subject to the same ethical and legal limitations that apply to its earthly roots.

Finally, harmonization enhances the stability of the system. As long as both norms of explainability, fairness, and oversight are in force on inter-jurisdictional levels, the issue, whether it is space law or AI law, will become procedural instead of substantive. Such a convergence is indicative of the governance of the twenty-first century, a global legal ecosystem whereby the policies and technologies of the earth and those of the orbit mutually support the same normative grounds.

Soft Law and Customary Evolution

On the one hand, the binding treaties are rather stable, but in many cases, they are formed after years of negotiations. Soft law, in turn, is made up of non-binding codes of conduct, best-practice guidelines, and voluntary

compliance frameworks, which may change more quickly and adaptively (Soroka & Kurkova, 2019). As a governance of AI in space, soft-law mechanisms can be regarded as the connective tissue that helps to maintain cooperation in the process of the long-term gestation of formal treaties.

Starting with the states, it is possible to implement codes of transparency and conduct of AI-enabled satellites, undertaking to publicize limited amounts of audit data, incident reports, and performance metrics. With time, the consistent compliance with these voluntary standards might be transformed into customary international law, once the consistent state practice is supplemented by a feeling of legal commitment (Pagallo, 2023). This process of normative consolidation is a reflection of the maritime law development, wherein in the initial stage voluntary safety codes were issued and later transformed into binding conventions under the International Maritime Organization (Galloway, 1981).

Innovation is also promoted by soft law. Its lack of punitive rigidity makes it open to experimentation with a variety of models of verification, cryptographic protocols, and institutional designs. The innovations that succeed can subsequently be enshrined with the help of annexes to the treaty or directives of SIA. Flexibility and formalization are related in a way that guarantees that the governance is dynamic with the technological rate of development of AI.

Lastly, trust diplomacy is encouraged by soft law. The interpersonal networks among the regulators, scientists, and military officers are built through joint announcements, joint workshops, and joint capacity-building programs. Such networks are able to spread the suspicion and develop a common language of responsibility. In this respect, soft law is not so transitional but a sociological basis of the eventual constitutionalization of AI-space government.

Conclusion

The nature of outer space has changed primarily due to the introduction of artificial intelligence, which, as a consequence, has transformed it from a passive area of observation to an intelligent ecosystem. The technologies that are currently orbiting the earth do not just pass information anymore; they interpret, decide, and take action. This change has identified the weaknesses of the current legal systems, which were developed during a time of human dominance and cannot be used to oversee the matters decided by complex and opaque intelligence systems that learn on their own.

This paper has proposed a reconstructed legal structure that can respond to these challenges. The layered sovereignty model redefines sovereignty as physical control, data custodianship, and algorithm custody, which are accountable in all aspects of intelligent space practice. These principles would be operationalized by institutional means like the Space Intelligence Authority (SIA) and the National AI Audit Bureaus (NAABs) by certification, inspection, and open-minded verification. The two, collectively, provide the procedural framework necessary for the maintenance of responsibility and duty without overshadowing innovation.

Based on the theories of fairness and auditability, the framework is balanced in terms of technological progress and the rule of law. It envisions a future when ethical and functional control of intelligent systems, instead of territory, would determine sovereignty beyond Earth. When authority is defined in terms of autonomy, the intersection of law and intelligent systems aligned, and the expansion of AI into outer space must strengthen the pillars of accountability and equity.

References

Abashidze, A. K., Gugunskiy, D. A., & Solntsev, A. M. (2022). International legal aspects of the use of artificial intelligence in outer space activities. *Space Policy, 61*, 101451.
Google Scholar Worldcat Fulltext

Abbasi, M. S., Munir, B., Jayaram, V., & Rivas, P. (2025). Leveraging autocorrelation in a dilated CNN-LSTM framework for predicting the US Supreme Court decisions. *IEEE Access.* https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=11162521
Google Scholar Worldcat Fulltext

Alarie, B., Niblett, A., & Yoon, A. H. (2016). How artificial intelligence will affect the practice of law. *University of Toronto Law Journal, 66*(1), 106–124. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3066816
Google Scholar Worldcat Fulltext

Bayern, S. (2015). The implications of modern business-entity law for the regulation of autonomous systems. *Stanford Technology Law Review, 19*, 93–112. https://law.stanford.edu/wp-content/uploads/2017/11/19-1-4-bayern-final_0.pdf
Google Scholar Worldcat Fulltext

Bratu, S., Popescu, G. H., & Gherghina, R. (2021). Artificial intelligence liability in autonomous systems: Legal gaps and policy implications. *Journal of Public Administration and Governance, 11*(3), 45–60.
Google Scholar Worldcat Fulltext

Burri, M. (2017). Understanding the accountability of autonomous systems. *Minds and Machines, 27*(3), 495–512.
Google Scholar Worldcat Fulltext

Carrillo, A. (2020). *Artificial intelligence and the future of global governance*. Oxford University Press.
Google Scholar Worldcat Fulltext

Chesterman, S. (2020). *We, the robots? Regulating artificial intelligence and the limits of the law*. Cambridge University Press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4231363
Google Scholar Worldcat Fulltext

Council of Europe. (2019). *Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes*. Strasbourg, France: Council of Europe. https://www.coe.int/en/web/data-protection/-/declaration-by-the-committee-of-ministers-on-the-manipulative-capabilities-of-algorithmic-processes
Google Scholar Worldcat Fulltext

CSET (Center for Security and Emerging Technology). (2025). *Artificial intelligence in orbital defense networks*. Washington, DC: Georgetown University.
Google Scholar Worldcat Fulltext

European Space Agency (ESA). (2018). *The future of space safety and sustainability: Space 4.0 and beyond*. Paris, France: ESA Publications. https://www.sdo.esoc.esa.int/environment_report/Space_Environment_Report_latest.pdf
Google Scholar Worldcat Fulltext

Friedland, G., & Lum, C. (1987). Satellite data systems and security architecture. *Journal of Spacecraft and Rockets, 24*(5), 375–383.
Google Scholar Worldcat Fulltext

Galloway, E. (1981). *The development of international law of the sea: Legal and institutional issues*. United Nations Institute for Training and Research.
Google Scholar Worldcat Fulltext

Gupta, R., Shukla, S., & Mishra, P. (2014). Big data in space exploration: A review of data management and sovereignty. *Acta Astronautica, 104*(2), 377–384.
Google Scholar Worldcat Fulltext

Hobe, S., Schmidt-Tedd, B., & Schrogl, K. U. (Eds.). (2013). *Cologne commentary on space law* (Vol. II). Carl Heymanns Verlag.
Google Scholar Worldcat Fulltext

Hu, J. (2024). AI and data sovereignty in outer space law. *Journal of Space Law, 49*(2), 221–242.
Google Scholar Worldcat Fulltext

Hu, J., Wang, L., & Torres, E. (2025). Machine learning architectures for orbital security systems. *Space Systems Review, 12*(1), 33–58.
Google Scholar Worldcat Fulltext

Irfan, M., Yasin, A., Hussain, R. A., Bashir, N., & Munir, B. (2024). ARTIFICIAL INTELLIGENCE, DATA PROTECTION AND TRANSPARENCY: A COMPARATIVE STUDY OF GDPR AND CCPA. *Journal of Media Horizons*, *5*(3), 76-85.
Google Scholar Worldcat Fulltext

Kopal, V. (1966). *Space law: Development and scope*. Martinus Nijhoff.
Google Scholar Worldcat Fulltext

Li, C. (2025). *Algorithmic liability in autonomous satellites. Journal of Space Policy and Technology, 15*(4), 101–128.
Google Scholar Worldcat Fulltext

Lin, P. (2012). *Autonomous military robotics: Risk, ethics, and design*. Office of Naval Research.
Google Scholar Worldcat Fulltext

Manheim, K., & Kaplan, L. (2019). Artificial intelligence: Risks to privacy and democracy. *Yale Journal of Law & Technology, 21*(1), 106–167. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3273016
Google Scholar Worldcat Fulltext

Moon Treaty. (1979). *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*. 1363 U.N.T.S. 21.
Google Scholar Worldcat Fulltext

Munir, B. (2025). *Artificial Intelligence for Lawyers: Navigating Novel Methods and Practices for the Future of Law*. Punjab Law Book House.
Google Scholar Worldcat Fulltext

Munir, B., Khalid, S., & Noreen, U. (2025). EXPOSING ISLAMOPHOBIA IN MACHINE LEARNING: A CRITICAL ANALYSIS OF THE EXISTING THEORIES AND BIASES. *Center for Management Science Research*, *3*(3), 1-9. https://doi.org/10.5281/zenodo.15173249
Google Scholar Worldcat Fulltext

National Security Commission on Artificial Intelligence (NSCAI). (2021). *Final report*. Washington, DC: U.S. Government Publishing Office.
Google Scholar Worldcat Fulltext

Novelli, T., Singh, P., & Rahman, S. (2024). Auditing AI in space systems: Verification protocols for orbital networks. *AI and Space Law Review, 3*(2), 51–73.
Google Scholar Worldcat Fulltext

Outer Space Treaty. (1967). *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*. 610 U.N.T.S. 205.
Google Scholar Worldcat Fulltext

Pagallo, U. (2023). *Law and the governance of artificial intelligence*. Springer. https://doi.org/10.1007/978-3-031-41264-6_13
Google Scholar Worldcat Fulltext

Raza A, Munir B, Ali G, Othi M A, & Hussain R A. (2024). BALANCING PRIVACY AND TECHNOLOGICAL ADVANCEMENT IN AI: A COMPREHENSIVE ANALYSIS OF THE US PERSPECTIVE. *International Journal of Contemporary Issues in Social Sciences*, *3*(3), 3732–3738. https://ijciss.org/index.php/ijciss/article/view/1653
Google Scholar Worldcat Fulltext

Raza, S. (2024). Fairness by design: Embedding equity into AI algorithms. *AI & Society, 39*(2), 215–229. https://doi.org/10.13140/RG.2.2.24957.58088
Google Scholar Worldcat Fulltext

Soroka, S., & Kurkova, E. (2019). Soft law in artificial intelligence governance: From ethics to regulation. *Computer Law Review International, 20*(6), 161–169.
Google Scholar Worldcat Fulltext

Tricco, M. (2025). AI-enabled defense intelligence: A legal perspective. *Defense & Security Review, 47*(2), 15–31.
Google Scholar Worldcat Fulltext

Wark, D. (2025). Satellites and national security in the AI age. *Journal of Strategic Studies, 48*(1), 99–118.
Google Scholar Worldcat Fulltext