http://doi.org/10.23925/2179-3565.2025v16i2p124-134

RISUS - Journal on Innovation and Sustainability
volume 16, número 2 - 2025
ISSN: 2179-3565
Editor Científico: Arnoldo José de Hoyos Guevara
Editor Assistente: Vitória Catarina Dib
Avaliação: Melhores práticas editoriais da ANPAD

SAFEGUARDING ORBITAL SUSTAINABILITY: ADDRESSING AI-DRIVEN SATELLITE DE-ORBITING BY NON-STATE ACTORS UNDER INTERNATIONAL LAW

Salvaguardando a sustentabilidade orbital: abordando a desorbitação de satélites impulsionada por ia por atores não estatais sob o direito internacional

Ashish Kakkar
Research Scholar, Gujarat National Law University, Gandhinagar, India
E-mail: ashishphd202306@gnlu.ac.in

ABSTRACT

The intersection of artificial intelligence (AI) and space security introduces unprecedented legal and operational challenges, particularly when non-state actors exploit AI to target critical space infrastructure. This paper examines the legal ramifications under international law of a scenario in which a navigational satellite is deliberately de-orbited through AI-enabled means by non-state actors. Existing agreements, such as the Liability Convention (1972) and the Outer Space Treaty (1967), provide fundamental structures but do not directly address the difficulties associated with attribution in cyberspace and the complexity of autonomous systems. The examination looks at the boundaries of fault-based accountability, state responsibility, and new due diligence guidelines in space governance. Particular focus is placed on the function of juridical and cyber law tools in mitigating AI-related risks. The paper concludes by advocating for the evolution of international legal instruments, incorporating AI-specific provisions, and establishing enhanced cooperative mechanisms to safeguard space assets from emerging non-traditional threats.

Keywords: Artificial Intelligence, De-orbiting, Outer space treaty, Liability convention, Cybersecurity

ACEITO EM: 09/05/2025
PUBLICADO: 20/06/2025

RISUS - Journal on Innovation and Sustainability
volume 16, número 2 - 2025
ISSN: 2179-3565
Editor Científico: Arnoldo José de Hoyos Guevara
Editor Assistente: Vitória Catarina Dib
Avaliação: Melhores práticas editoriais da ANPAD

SALVAGUARDANDO A SUSTENTABILIDADE ORBITAL: ABORDANDO A DESORBITAÇÃO DE SATÉLITES IMPULSIONADA POR IA POR ATORES NÃO ESTATAIS SOB O DIREITO INTERNACIONAL

Safeguarding orbital sustainability: addressing ai-driven satellite de-orbiting by non-state actors under international law

Ashish Kakkar
Research Scholar, Gujarat National Law University, Gandhinagar, India
E-mail: ashishphd202306@gnlu.ac.in

RESUMO

A interseção da Inteligência artificial (IA) e da segurança espacial introduz desafios legais e operacionais sem precedentes, particularmente quando atores não estatais exploram a IA para atingir a infraestrutura espacial crítica. Este artigo examina as ramificações legais sob o direito internacional de um cenário em que um satélite de navegação é deliberadamente desorbitado através de meios habilitados para-IA por atores não estatais. Os acordos existentes, como a Convenção de Responsabilidade Civil (1972) e o Tratado do espaço exterior (1967), fornecem estruturas fundamentais, mas não abordam diretamente as dificuldades associadas à atribuição no ciberespaço e a complexidade dos sistemas autônomos. O exame analisa os limites da responsabilidade baseada em falhas, responsabilidade do estado e novas diretrizes de Due diligence na governança espacial. Um foco Particular é colocado na função das ferramentas jurídicas e de direito cibernético na mitigação de riscos relacionados à IA. O documento conclui defendendo a evolução dos instrumentos jurídicos internacionais, incorporando disposições específicas de IA e estabelecendo mecanismos cooperativos aprimorados para proteger os ativos espaciais de ameaças não tradicionais emergentes.
Palavras-chave: Inteligência Artificial, Desorbitação, Tratado do espaço sideral, Convenção de responsabilidade civil, Cibersegurança

INTRODUCTION

The rapid evolutionary progression of artificial intelligence (AI) has made a huge impact on the domain of outer space. Today, satellites that used to be controlled only by manual or semi-automated systems are becoming more and more reliant on AI-based navigation, threat detection, and orbital adjustment. Advancements like these make operations more efficient but also make these operations vulnerable to malicious actors. Potential for misuse of AI by non-state actors to target space assets, namely navigational satellites, that are central to providing civilian and military service.

This study examines what is otherwise hypothetical but has become increasingly plausible, and studies what it means for a navigational satellite to be intentionally de-orbited by nonstate actors using methods enabled by AI. An example of such an event could be cyber intrusions or alteration of the control loop of a satellite, or the deployment of an autonomous system capable of interfering with a satellite's trajectory. This scenario is intricate and its permissible inferences are untested in international law that includes state responsibility, attribution, and liability.

Although the two cornerstones of the international legal regime governing space activities are the Convention on International Liability for Damage Caused by Space Objects (the Liability Convention) of 1972 and the Outer Space Treaty (OST) of 1967, the former defines liability standards for damage caused by space objects, and the latter establishes state responsibility for national space activities, other important and recent pieces of international law influence space activities. The treatment of these treaties was when AI or heavily trained nonstate actors could do space-related things. Also, there is a large normative difference between how AI's dual-use characteristics are managed and the attributional problems it presents.

The main purpose of this paper is to critically discuss the competence of the existing worldwide legal instruments to deal with the misuse of AI in space by non-state actors. It will analyze legal doctrines including state responsibility, due diligence, and international cooperation, as well as ascertain the validity of cyber norms and soft law developments. Using this inquiry, the study intends to contribute to the nascent discussion regarding the governance of AI in outer space by outlining reforms to international law that would strengthen deterrence and accountability in this evolving domain.

1 THEORETICAL BACKGROUND

1.1 Regional Dynamics: The Indo-Pacific Space Race and Emerging Security Challenges

In recent years, the Indo-Pacific has become a single crucial point in the global struggle for space dominance whereby satellite capabilities, space exploration programs, and the militarization of space assets are in rapid advance. Satellite infrastructure is being heavily invested in by key regional actors like China, India, Japan, Australia, and South Korea, not only as a civilian but also as a military tool that is integrated with artificial intelligence. The lack of legal harmonization or a shared security framework means that this regional acceleration is not matched by support for making the region vulnerable – especially to nonstate actors, using AI.

1.2 Rise of Dual-Use Technologies and AI Integration

Dual-use space technologies are increasingly being deployed by the Indo-Pacific states that offer systems that can be used for both civilian and military purposes. India, China, and Japan's development of navigational satellite constellations such as India's NAVIC, China's BeiDou, and Japan's QZSS are examples of navigational satellite constellations developed with high strategic utility. Such systems usually involve AI for such functions as autonomous orbit management, anomaly detection, and security. Increasing the resilience to AI comes at the price of creating new vectors for attack. The feasibility of redirecting or deorbiting a satellite by a non-state actor compromising an AI-powered subsystem would have serious regional security and economic stability implications.

RISUS – Journal on Innovation and Sustainability, São Paulo, v. 16, n. 2, p. 124-134, maio/jun. 2025 - ISSN 2179-3565

1.3 Absence of Regional Legal Mechanisms

The Indo-Pacific is unlike the European Union where broader space governance initiatives and cybersecurity directives like the EU Code of Conduct for Outer Space Activities have been developed and while there are no binding regional legal instruments to regulate outer space activities or AI-based security threats. There are no suits in the existing multilateral dialogues like ASEAN Regional Forum or QUAD yet with space law or governance of the AI, so to speak. The outcome is a break in the legal landscape so that attribution, jurisdiction, and cooperation response mechanisms remain scarce.

1.4 Escalating Risk of Asymmetric Threats

Asymmetric threats by non-state actors in the Indo-Pacific are greater in the context of the legal vacuum. For example, if a nonstate group could be provided or relied on for operational AI to disrupt or de-orbit a regional satellite creating cascading geopolitical tensions. With the density of space assets in Low Earth Orbit (LEO) in the region, the risk of debris generation and collateral damage is greater and may affect third-party states not partaking in the original act. In such a case, the difficulty of attribution and the absence of regional legal recourse would make it difficult to respond to such a scenario under the Outer Space Treaty[3] or the Liability Convention.

1.5 A Path Toward Regional Legal Harmonization

Given these vulnerabilities, it is imperative to harmonize the law proactively in the Indo-Pacific. Under the aegis of the QUAD or ASEAN, a regional code of conduct for the use of AI in space on the lines of the EU Code of Conduct could be facilitated. A framework of such a kind could include mutual legal assistance provisions in investigating AI-led space incidents, agreement on shared attribution standards for cyber interference with space assets, joint threat assessments and AI verification protocols, emergency response coordination, and debris mitigation agreements. Where soft law approaches exist without such legally binding instruments, they can fill in for a basis for trust and cooperation as they aspire to lead towards the formation of more formalized regional treaties.

1.6 National Approaches to Space and AI Governance in the Indo-Pacific

1.7 India: Strategic Ambiguity and Expanding Military Capabilities

Past India's space governance has been focused on peaceful use of space, but this is changing as space is increasingly viewed as a strategic domain. India became the latest entrant in the small club of nations that have demonstrated offensive counterspace capabilities with its 2019 Mission Shakti anti-satellite (ASAT) test. Even though India has not adopted a separate space law, the country has drafted a law that regulates commercial space activities in India but does not contain any provisions about AI and cyber threats.

Keeping in mind the AI focus, one is the National Strategy for Artificial Intelligence developed by NITI Aayog in 2018 which is a general approach for responsible AI and does not discuss space-specific applications or dual-use concerns. Integrated response to the space and cyber threats in India is complicated by the siloing of space and cyber governance. India's legal architecture for addressing AI-enabled space threats is, however, reactive rather than anticipatory, though India participates in international forums.

1.8 China: Strategic Integration of AI and Space in National Defense

Space is considered by China as an integral part of its national security plan. The 2019 White Paper on China's National Defense specifically lists space as a critical area of security. The BeiDou satellite navigation system has been proven to be vital to Chinese military command and control infrastructure and is equipped with AI capabilities for autonomous orbit control and signal optimization.

Despite this, China has, legally, not published a comprehensive space law covering security issues, cybersecurity, and data governance laws such as the Cybersecurity Law (2017) and Data Security Law (2021) which give extensive powers of regulation over critical infrastructure, i.e. space assets. The laws blur the distinction between the use of science and technology in civilian and military applications of science and technology and enhance state control over private innovation. The question is raised as to transparency and accountability when AI-enabled attacks come out of or inside of China's tight regulated environment.

1.9 Japan: Dual Commitment to Technological Leadership and Legal Restraint

Japan has a relatively transparent and rule-based legal framework that combines powerful technological capabilities. It has two supporting legal frameworks, namely the Basic Space Law (2008) and the Space Activities Act (2016) which serve as guidelines to all public and private space activities to be safe, and transparent and shall comply with its international obligations. Similar to Japan, space is integrated into the national security architecture of Japan through the creation of the Japan Self-Defense Forces Space Operations Squadron (2020).

Japan is one of only a few Indo-Pacific countries openly discussing normative issues in the fields of AI and space governance. The AI Governance Guidelines (2021) encourage the principles of accountability, transparency, and oversight by humans, among others, in the deployment of AI. They are, however, nonbinding, but provide a model for regional soft law instruments. The calls for a regional framework to mitigate risks derived from potential misuse of AI in space, Japan's intervening participation in the most advanced form of technological advancement such as the G7, the QUAD, and the Artemis Accords shows its function as a bridge between technological progress and legal responsibility.

1.10 Synthesis: divergent legal cultures, converging risks

While India, China, and Japan each possess distinctive legal philosophies, governance models, and strategic priorities, they have a common vulnerability to AI-enabled space asset threats. By not binding with regional norms and inconsistent national legal protections that limit AI misuse, it lapses with a regulatory void that nonstate actors might undertake. The more regional powers invest in autonomous and dual-use systems of satellites, the greater the risk of unregulated deployment of AI, whether malicious or accidental, will be.

The two are legal and strategic divergence and there is an urgent need for a multilateral Indo-Pacific framework that would put national policies in line, promote transparency, and promote collective security in outer space. It discusses how international legal doctrines can help, or not, Windows the applicability of the international legal framework in areas of space governance, as well as making the scope for incorporating AI-specific safeguards.

1.11 Legal framework analysis

Presently, the legal framework for space operations is largely the result of Cold War agreements, well before non-state actors and AI development. Even though the Outer Space Treaty (OST) and the Liability Convention are still fundamental, they were not intended to address the complex interactions between the decentralized actors, autonomous systems, and cyber operations. This section asks whether the current legal framework can manage a satellite de-orbiting that is facilitated by AI and directed by non-state actors. The paper focuses on the Outer Space Treaty, Services Convention, Liability Convention, Cybersecurity and AI Law, and the Role of State Responsibility.

1.12 Outer Space Treaty

As Article VI of the Outer Space Treaty states, governments are responsible worldwide for activities of their national space operations, including those by nongovernmental organizations. As such, states are under a

positive obligation to approve and regulate nonstate activity. Even if a state had no direct knowledge or intent, it could be internationally responsible if a private firm or non-state actor within a state's jurisdiction de-orbits a satellite using AI tools in principle.

But the problem is that the actors are clandestine, decentralized, or use forged digital identities, which is the case both in cyber and AI based threats. Such cases make proving effective jurisdiction or control considerably more difficult. Although implicit in Article VI, the scope of AI under the principle of 'due diligence' is unclear and creates a gap in accountability and enforcement.

1.13 Liability Convention

According to Article II of the Liability Convention, absolute liability is liable for damage to aircraft or the Earth's surface, while Article III prescribes that fault-based liability is liable for harm occurring anywhere in space. One would be a de-orbiting attack that damaged in orbit other satellites causing debris, and that would have to prove fault. When the action is born out of an autonomous system, the establishment of fault is especially tricky, especially if the AI is self-learning or simply unpredictable due to algorithmic complexity.

The Convention does not address the responsibility of nonstate actors themselves. If the actor has state accountability, invocation of state accountability is possible if the actor can be traced to a state. The existence of divergence of state accountability due to a lack of direct enforcement instruments and dispute settlement procedures. In particular, if a nonstate actor cannot be unequivocally linked to a state, that state may not have an easy route to restitution or penalties.

1.14 Cybersecurity and AI Law

Generally, imitating the Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA), international law is state-centric as far as attribution doctrines are concerned. These are notoriously difficult to achieve in cyber operations as they require clear evidence of state control or direction. In AI-driven environments with autonomous systems, the difficulty is added in. As nonbinding, the Tallinn Manual 2.0 acknowledges the difficulties of applying the laws of armed conflict and state responsibility to foreign cyber operations involving nonstate actors and autonomous systems.

Since there are no AI-specific attribution criteria, this gap cannot be filled at all, as hostile actors leverage it to avoid accountability. If there are no clear norms or legal standards of how to develop, deploy and supervise AI, there is potential for both malicious and accidental misuse to escape traditional Doctrine of Responsibility.

1.15 Role of State Responsibility

Any discussion of accountability in space law must necessarily concern state responsibility. The Outer Space Treaty contains broad obligations, but blanks remain when and how to hold a state accountable for acts of AI by private or decentralized entities. Decisive are issues of effective control and knowledge. If an AI system does not act under human supervision, the legal basis for attributing its behavior to a particular state becomes murky. It is particularly acute in geopolitical sensitive regions such as Indo-Pacific where states may have implicit motives to allow or indirectly back proxy actors.

Partial avenues to the establishment of responsible behavior are provided by soft law and normative frameworks such as UN Guidelines for the Long-Term Sustainability of Outer Space Activities and various draft codes of conduct. But they are neither binding nor sufficiently detailed to fill the doctrinal gaps regarding AI-enabled sabotage. Thus, the question of the state's responsibility in AI-driven space incidents remains open in international law.

1.16 Challenges in attribution and enforcement

It is now widely recognized that one of the most pressing issues of international law is the capacity to apply legal norms to space and cyber operations involving AI. If non-state actors use AI to de-orbit a navigational satellite and then some autonomous decision-making and some advanced obfuscations, it will reveal weaknesses in existing legal and operational means for enforcement. Various factors related to interrelated factors make it difficult to hold perpetrators accountable or to compel preventive measures.

1.17 Evidentiary and Technical Complexities

To attribute AI-enabled operations using a reliable chain of evidence requires the evidence to be able to link the event to a specific actor, location, or command origin. In the cyber domain, spoofing, encryption, anonymization and the use of proxy networks already make attribution difficult. In space, satellite operations are transnational, and proprietary AI systems used for control or navigation are opaque to the observer, and these obstacles are further magnified. An AI system that has been trained to run itself, to act in the real world, and to adapt to new contexts may not implement explicit human intent at the moment of execution.

1.18 Jurisdictional and Legal Obstacles

The Outer Space Treaty is based on the principle that launching states and states of registration have authority and control over space objects. The modern satellite missions frequently involve many states working together or contracting private entities across borders and it becomes challenging to determine which state has the ultimate jurisdiction. Space law still lacks extraterritorial enforcement for the most part and this remains true today, although there is no universal legal mechanism that is comparable to the International Criminal Court for the punishment of international space law violations. Indeed, only the inter-state disputes are arbitrable - by the International Court of Justice (ICJ) and Permanent Court of Arbitration (PCA), whereas there are no such standing procedures in place in cases brought against non-state actors.

1.19 Non-State Actors and the Accountability Void

In particular, current space treaties do not address the legal status or liability of non-state actors. The Outer Space Treaty Article VI requires state approval and administration of nongovernment entities, but this presumes a state level of awareness and control that is often lacking in clandestine or hostile operations. When groups are covert, decentralized, and involve the use of AI, the line between negligence, tacit support and no ability to control becomes blurred. This gray zone creates plausible deniability and makes it harder to deter and retributive in the international system.

1.20 Inadequacy of Existing Dispute Resolution Mechanisms

The current international space law provides limited scope and practicality to dispute resolution. The Outer Space Treaty contains no binding enforcement provisions about Article IX, which calls for consultation in cases of harmful interference. While the Liability Convention specifies the procedures for claims, it has never been tested for complex AI-related sabotage cases. Even if fault can be established, the question remains whether such compensation or injunctive relief can be practically enforced.

1.21 Normative Gaps and Strategic Ambiguity

A final strike is that there is no agreement about how to regulate emerging technologies such as AI in a space activity environment. There are no uniform global AI Auditing, Cybersecurity protocols, or autonomous Sunsets on satellite availability and behavior. This is because states may be reluctant to impose strict rules that

prevent them from developing their technology or its military applications. The fertile ground that gray zone activities provide for state and nonstate actors to operate in, means rebel and state actors alike leave potential victims and third parties with very little legal recourse.

2 CASE SCENARIOS OR HYPOTHETICAL ANALYSIS

2.1 Hypothetical Scenario: The De-Orbiting of SatNav-X

To bring these out in practice, take a situation where India and a consortium of Indo-Pacific private space companies' joint operating critical regional navigation satellite, SatNavX, departs suddenly from its geosynchronous stable elliptical orbit. The satellite enters back into Earth's atmosphere within hours, where it is destroyed over the Indian Ocean. The investigations show that unauthorized access was made to SatNav-X's AI-based autonomous orbit management system. To introduce malware, incremental trajectory shifts were introduced that mimicked legitimate AI protocols. It is traced to an international nonstate actor, Shadow Vector, with signs of logistical support from servers hosted in a neutral third state.

The de-orbiting disrupts civilian air traffic control and maritime positioning, leading to a collision between a Japanese cargo vessel and a commercial ship. Economic losses mount, and tensions rise as India and Japan protest in international forums. Yet no official attribution to a specific state is made, and no established mechanism compels Shadow Vector to face liability.

2.2 Legal Analysis of the Scenario

Attribution and State Responsibility: Under Article VI of the Outer Space Treaty, India could be held globally responsible for the activities of non-governmental entities it supervises. However, the perpetrator appears external and clandestine. Without proof of effective control by any state, the event falls into a legal vacuum where conventional doctrines of state responsibility under ARSIWA may not apply.

2.3 Liability Under the Liability Convention:

Article III of the Liability Convention imposes fault-based obligation for damage in outer space. India, as a launching state, could theoretically be liable if negligence in AI supervision is proven. Yet the sabotage originated from an external non-state actor. Absent a showing of fault or due diligence failure, India might evade liability, leaving victim states with no clear avenue for redress.

Role of Due Diligence and Cybersecurity Standards: The open question is whether India and its private partners met their due diligence obligations so far as safeguarding AI systems is concerned. It is difficult to prove negligence as AI safety or cybersecurity in satellite operations has to be established as an international baseline. If India used reasonable care, the absence of global AI standards for space assets indicates a normative gap that serves to threaten accountability.

Gaps in Dispute Resolution: There is no binding regional framework and no effective global tribunal to address such incidents in which non-state actors are involved. Under the Optional Rules for Space Disputes of the PCA, arbitration would be necessary only with mutual consent, which is unlikely in case of a clandestine attack. Bilateral agreements concerning forensic cooperation may be reached through diplomatic means, but they will not obtain liability or restitution. It brings to the fore the strategic ambiguity and enforcement void that AI-empowered threat engenders. SatNav-X will likely become more frequent unless stronger cybersecurity standards, clearer liability rules, and meaningful attribution protocols are established.

3 POLICY AND LEGAL RECOMMENDATIONS

The challenges described above show that for an area as potentially devastating as that of satellites aided by AI, the existing international legal framework is unable to cope. In this section, the potential for a multi-layer

of recommendations is proposed about the clarification of legal obligations, enhancing cooperation, codification of AI standards, building capacity as well as developing of robust compliance mechanisms.

3.1 Clarifying State Obligations in AI-Space Contexts

International space law must evolve to define the contours of due diligence and supervision obligations in the context of AI deployment. Article VI of the Outer Space Treaty could be interpreted—through soft law initiatives or revised treaty commentaries—to require states to conduct pre-launch AI safety assessments, mandate override capabilities, and implement third-party audits of AI algorithms for privately operated space systems.

3.2 Enhancing Multilateral and Regional Cooperation

Given the transnational nature of AI-enabled threats, enhanced cooperation is essential. An Indo-Pacific Regional Space-AI Governance Framework, facilitated by forums like the QUAD or ASEAN, could set shared attribution standards, improve forensic data-sharing, and establish joint threat monitoring cells modeled on the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

3.3 Codifying AI Standards in International Space Law

A dedicated protocol or soft-law annex to the Outer Space Treaty focusing on AI risks would address cybersecurity requirements, permissible autonomy thresholds, and failsafe protocols. This effort could draw inspiration from the Tallinn Manual's non-binding approach in cyber law, eventually paving the way for more binding instruments.

3.4 Building Technical and Legal Capacity

Small Indo-Pacific states, in particular, cannot regulate AI or probe sophisticated cyber intrusions in space systems. The capacity building of regulators and the formation of better local forensic capacity, local law clinics, or regional research centers in the AI space governance space can also be done on a targeted basis.

3.5 Establishing Accountability and Compliance Mechanisms

Preventive transparency and enforceable post-incident measures are crucial for further enhancing accountability for AI-enabled attacks. Mandatory disclosure regimes of the type of data breach notification laws could impose a duty upon operators to disclose AI anomalies and suspected breaches of cyber security. There could be independent attribution panels of technical and legal experts who issue findings in contested incidents in the domain of artificial intelligence, which would help judge responses in the diplomatic arena and then in the space of legal doctrines. Finally, it would be appropriate to amend or supplement the Liability Convention to include algorithmic accountability to bolster the legal framework.

CONCLUSION

Artificial intelligence, as a twin-use technology in space operations, is an invincible challenge to existing international legal regimes. International space law is so weak it acknowledges that when nonstate actors use AI to attack critical space infrastructure, for example deorbiting a navigational satellite, it becomes so complicated and complex that they cannot address the legal, strategic, and technological problems. Since the base instrument, the Outer Space Treaty and the Liability Convention is far from preparing for AI autonomy, the decentralized threat actors, or the transboundary cyber, offers are inadequate.

The scenario of SatNav-X is a hypothetical situation of huge difficulty in attributing responsibility, establishing liability, and securing legal remedies for AI driven sabotage. Such normative gaps, coupled with geopolitical sensitivities in the Indo Pacific such as differing legal cultures and differing strategic imperatives, make it especially challenging to overcome these challenges.

To address these vulnerabilities a multi-pronged approach is needed that includes clarifying and updating treaty obligations related to AI, developing cybersecurity and AI standards, increasing forensic and attribution capabilities, and building strong compliance and accountability mechanisms. There can be valuable stepping stones in the form of regional codes of conduct and capacity-building initiatives, although a more comprehensive framework would be the targeted treaty amendment or protocol.

In the end, AI in space has to be dealt with in ways that international law cannot keep up with. This failure may undermine issues of global stability and prosperity and could give rise to a strategic and a legal vacuum in an arena that is becoming more important by the day. The proactive development of the legal risks and implications posed by AI enabled satellite threats will benefit the global community as they strive to ensure that outer space remains a peaceful and sustainable environment in which to operate for generations to come.

REFERENCES

Cabinet office (Japan), AI Governance Guidelines (2021). https://www8.cao.go.jp/cstp/english/
Convention on International Liability for Damage Caused by Space Objects (adopted 29 March 1972, entered into force 1 September 1972) 961 UNTS 187 (Liability Convention).
Eichensehr, Kristen E. (2017). Eichensehr, Cyberattack Attribution and International Law, 95 Texas Law Review 1455.
European Union External Action Service (n 2).
European Union External Action Service, EU Code of Conduct for Outer Space Activities (2008).
Government of India, Draft Space Activities Bill. (2017). https://www.isro.gov.in/
Government of Japan, Basic Space Law (Law No. 43 of 2008); Space Activities Act (2016). https://www8.cao.go.jp/space/
Hollis, Duncan B., Benthem, Tsvetelina van (2022). Attribution by Algorithm: Artificial Intelligence and the Law of State Responsibility ,117 AJIL Unbound 154.
International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, UNGA Res 56/83 (12 December 2001).
Jakhu, Ram S., Pelton, Joseph N. (2017). Global Space Governance: An International Study.
Japan Ministry of Defense, Establishment of the Space Operations Squadron (2020). https://www.mod.go.jp/e/
Marchant, Gary E. et al. (2011) International Governance of Autonomous Military Systems: Ensuring Human Responsibility, 30 Columbia Science and Technology Law Review 1. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1778424
Ministry of External Affairs (India) (2019). Press Statement on Mission Shakti. https://mea.gov.in/
NITI Aayog, National Strategy for Artificial Intelligence: #AIforAll (2018) https://www.niti.gov.in/
Organisation for Economic Co-operation and Development (OECD), Principles on Artificial Intelligence (2019).
Permanent Court of Arbitration, Optional Rules for Arbitration of Disputes Relating to Outer Space Activities (2011) https://pca-cpa.org
Schmitt, Michael N. (Ed) (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.
Shaw, Malcolm N. (2021) International Law, Cambridge University Press, 9 ed., 796–802. https://assets.cambridge.org/97811084/77741/frontmatter/9781108477741_frontmatter.pdf
Standing Committee of the National People's Congress, Cybersecurity Law of the People's Republic of China (2017) http://www.npc.gov.cn/
Standing Committee of the National People's Congress, Data Security Law of the People's Republic of China (2021) http://www.npc.gov.cn/

State Council Information Office (China), China's National Defense in the New Era (2019) http://english.www.gov.cn/
Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (adopted 27 January 1967, entered into force 10 October 1967) 610 UNTS 205 (Outer Space Treaty).
United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS), Guidelines for the Long-Term Sustainability of Outer Space Activities, UN Doc A/AC.105/2019/CRP.7 (2019).
Weeden, Brian, Samson, Victoria. (2019). *Global Counterspace Capabilities:* An Open-Source Assessment. Secure World Foundation.