CYBER-ATTACKS IN OUTER SPACE: AI-DRIVEN WARFARE AND INDIA'S ROLE IN SHAPING LEGAL NORMS

Anirudh Sharma**,** BA LLB**,** Chaudhary Charan Singh University

ABSTRACT

Recent incidents show that the outer space is increasingly vulnerable to cyber-attacks. In 2022, thousands of satellite modems ("KA-SAT") were disrupted by a ransomware attack linked to state-sponsored actors[1]. Similarly, SpaceX reported jamming of Starlink terminals in Ukraine, underscoring the feasibility of electronically targeting satellites[2]. These events expose gaps in the Cold-War era legal regime: the 1967 Outer Space Treaty (OST) and 1972 Liability Convention were drafted before cyber threats or AI-enabled systems were envisioned[3]. In particular, OST relies on human consultation (Article IX) and liability for physical damage, neither of which easily accommodates fast, autonomous cyber-attacks. Scholars note the Liability Convention's "blind spot" it holds a launching state strictly liable for harm on Earth regardless of causation, meaning an innocent state could bear the cost of damage caused by a third-party cyber hijacker[4]. Meanwhile, autonomy and AI in space exacerbate complexity: US plans for fully autonomous satellites highlight how AI can help evade attacks (by altering orbits, detecting hacks, etc.),[5] but also raise questions of responsibility when AI makes split-second decisions absent human oversight[6]. This article examines these challenges, assesses India's legal measures (e.g. the IT Act 2000, the new Digital Personal Data Protection Act 2023, and a draft Space Activities Bill) and diplomacy (G20 space initiatives, COPUOS contributions, GPAI membership) aimed at securing space assets.

[1] Viasat KA-SAT attack (2022) - International cyber law: interactive toolkit
https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_(2022)
[2] Cyberattacks on Satellites
https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites
[3] The Outer Space Treaty
https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html
[4] Closing the Liability Loophole: The Liability Convention and the Future of Conflict in Space | Chicago Journal of International Law
https://cjil.uchicago.edu/print-archive/closing-liability-loophole-liability-convention-and-future-conflict-space
[5] AI Could Help the US Evade a Crippling Cyber Attack on Its Satellites - Business Insider
https://www.businessinsider.com/ai-could-help-us-satellites-evade-crippling-cyber-attack-china-2025-2
[6] Autonomy Has Outpaced International Space Law – War on the Rocks
https://warontherocks.com/2025/03/autonomy-has-outpaced-international-space-law

We explore proposals from online dispute-resolution (ODR) fora to a "Space Geneva Convention" to modernize the legal framework.

Emerging Cyber Threats in Space

Outer space is now a domain of cyber conflict as well as traditional space operations. On 24 February 2022, a massive cyber-attack (the KA-SAT incident) disrupted tens of thousands of Viasat satellite modems across Ukraine and Europe. The attack, widely attributed to a Russian military intelligence unit, encrypted user modems and knocked Ukrainian military units offline. Significantly, the attacker reached KA-SAT ground infrastructure (likely by compromising a VPN credential) and executed a wiper rather than ransom campaign[7]. Although the KA-SAT attack did not physically destroy the satellite itself, it temporarily severed essential communications. Similar incidents have arisen elsewhere: SpaceX's Starlink terminals sent to Ukraine were found being jammed in March 2022, and GPS spoofing or denial incidents have been reported against maritime and military navigation systems. These events demonstrate that satellites and ground stations are attractive targets. As digital infrastructure, they can be paralyzed or controlled by remote cyber means, potentially without any kinetic strike. Walter Peeters et al. observe that "cyberattacks on satellite systems has become increasingly real," noting SpaceX's experience in Ukraine. The ICRC similarly warns that an attack on satellite systems threatens civilian life-support: it notes that a cyber-operation against a satellite used for essential services (navigation, communication or remote sensing) puts civilians at risk. In short, cyber-attacks in space can cut off navigation, communications, and data relied upon by civilian economies and humanitarian actors[8].

Limitations of the Existing Legal Regime

The core international space treaties predate cyber operations, so they leave legal gaps. The 1967 Outer Space Treaty (OST) sets broad principles: space is free for exploration, not subject to national appropriation, and to be used for peaceful purposes[9]. It bars placing weapons of mass destruction in orbit and holds states responsible for "national activities in outer space" whether by government or private entities. OST Article VI, for example, makes states

[7] Viasat KA-SAT attack (2022) - International cyber law: interactive toolkit
https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_(2022)
[8] Cyberattacks on Satellites
https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites
[9] The Outer Space Treaty
https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html

"responsible" for non-state space actors. OST Article VII makes states "liable for damage" caused by their space objects[10]. However, OST assumes operators make decisions slowly enough to consult (Article IX), and that "harmful interference" means physical or radio interference, not cyber intrusions. Modern autonomous systems can alter orbits in milliseconds, leaving no time for the "international consultations" Article IX envisages, which assumed clear human decision chains[11]. Thus, OST provides no rule for an automated satellite suddenly moving to avoid an oncoming object without warning.

Similarly, the Convention on International Liability for Damage Caused by Space Objects (1972) imposes a strict liability regime for physical damage on Earth. Article II of that Liability Convention makes a "launching State" absolutely liable for any damage caused on Earth by its space object. Yet the Convention limits compensation to "loss of life, personal injury or impairment of health; or loss of or damage to property". It says nothing about economic loss from disrupted services, or damage not manifesting as physical loss. Critically, it applies only to physical harm on Earth (or to aircraft)[12], and it imposes liability on the state that launched the object regardless of how damage occurred. Hence, if a satellite was hijacked via cyber means and then crashed, the launching state would pay under strict liability even if it was an innocent victim of hacking. Law scholars note this is a paradox: an innocent launching state would "foot the bill for any damage caused by unknown culprits or third parties". This "blind spot" contravenes basic principles of state responsibility, and indeed conflict-of-laws analogies (such as the law of the sea) expect causation to matter. In sum, the Liability Convention does not inquire into the cause of the incident[13].

The net result is that none of the five UN space treaties directly addresses cyber-hacks or AI weaponization. Space objects are defined by their physical components[14] , not by onboard software; the treaties' language targets collisions and radio interference, not remote code exploits. A recent analysis concludes that "the Liability Convention is insufficient to cover all

[10] The Outer Space Treaty
https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html
[11] Autonomy Has Outpaced International Space Law – War on the Rocks
https://warontherocks.com/2025/03/autonomy-has-outpaced-international-space-law
[12] Liability Convention
https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/liability-convention.html
[13] Closing the Liability Loophole: The Liability Convention and the Future of Conflict in Space | Chicago Journal of International Law
https://cjil.uchicago.edu/print-archive/closing-liability-loophole-liability-convention-and-future-conflict-space
[14] Liability Convention
https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/liability-convention.html

cyber threats" because it was never meant to address virtual or data-based harms[15]. In practice, there is no international rule clarifying, for example, whether jamming a satellite's ground station constitutes a "use of force" or a violation of peacetime obligations. In fact, as Patricia Lewis (Chatham House) observes, "There is no rules-based order in place that is fit to deal with cyber attacks" on space systems. Likewise, India's own COPUOS statements underline that no legally binding instrument currently governs cyber activity in space, and urge the development of such norms[16].

AI, Autonomy, and the New Complexity

Artificial intelligence and autonomous satellites further strain the old rules. Modern missions rely on machine learning for debris tracking, navigation and on-board decision-making. The US Space Force predicts that by 2035 most space operations will be heavily autonomous. Indeed, Defense Department programs like DARPA's Blackjack aim to field satellite constellations that self-coordinate and react to threats with little human input. In 2024 Oman launched an AI-enabled remote-sensing satellite for real-time processing, and SpaceX reports performing tens of thousands of automatic collision-avoidance maneuvers in months[17]. Autonomous satellites can adapt more quickly than ground crews to challenges. As Business Insider notes, AI-driven "decentralized decision-making may add resilience by decreasing reliance on ground-based infrastructure" and "help satellites better understand what other satellites are doing". In other words, AI can help satellites evade jamming or plot around hostile actors faster than a human operator could respond[18].

While autonomy brings defensive advantages, it also complicates legality and cybersecurity. If multiple AI-driven satellites make independent maneuvers, "harmful interference" could occur by accident – for instance if one AI system inadvertently causes orbital congestion. The OST's consultation framework is outdated for seconds-long automated decisions[19]. Moreover, AI can

[15] Liability for Cyber Attacks on Space Objects by Anna Hurova :: SSRN
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3835760
[16] Create a Global Code of Conduct for Outer Space | Chatham House – International Affairs Think Tank
https://www.chathamhouse.org/2019/06/create-global-code-conduct-outer-space
[17] Autonomy Has Outpaced International Space Law – War on the Rocks
https://warontherocks.com/2025/03/autonomy-has-outpaced-international-space-law/
[18] AI Could Help the US Evade a Crippling Cyber Attack on Its Satellites - Business Insider
https://www.businessinsider.com/ai-could-help-us-satellites-evade-crippling-cyber-attack-china-2025-2
[19] Autonomy Has Outpaced International Space Law – War on the Rocks
https://warontherocks.com/2025/03/autonomy-has-outpaced-international-space-law/

be targeted. An autonomous satellite's own decision-making software could be hacked or spoofed, leading it to behave erratically. China's 2023 leaked CIA report warned that adversaries may attempt "to hack the systems used to control US satellite networks" as a tactic of modern warfare[20]. AI thus broadens the attack surface: adversaries might deploy their own AI-driven space systems (even cyber-satellites programmed to disrupt others) or use machine learning to coordinate multi-vector assaults (e.g. cyber plus electronic jamming).

Legally, AI raises hard questions of responsibility. If an AI satellite "decides" to collide or disables another satellite via a cyber-weapon, who is the actor? The Outer Space Treaty imposes state responsibility for any space activity, but AI blurs the line between a system's action and its owner's intent. War on the Rocks commentary highlights that current law lacks a definition of when an automated maneuver triggers liability, and urges that liability attach to states whose licensed operators deploy AI systems[21]. The Tallinn Manual series (on cyber warfare) touches on space, but acknowledges "data spoofing and cyber hacking in space exist in far murkier legal frameworks"[22]. In sum, AI-driven spacecraft create a world that the drafters of 1960s-era treaties could not have imagined, revealing the urgent need to update norms for "AI in orbit."

India's Legal and Policy Initiatives

India is actively modernizing its space and cyber laws, and pushing for stronger international rules. Domestically, the Information Technology Act 2000 (as amended) criminalizes various cyber offenses, including Section 66F which defines "cyber terrorism" as acts intended to threaten India's security (e.g. hacking intended to "strike terror" or deprive authorized access)[23]. Offenders face life imprisonment. These provisions are broad and could apply to hostile cyber-operations against satellites or space infrastructure. India has also enacted a new Digital Personal Data Protection Act (DPDP Act 2023), which establishes safeguards for

[20] AI Could Help the US Evade a Crippling Cyber Attack on Its Satellites - Business Insider
https://www.businessinsider.com/ai-could-help-us-satellites-evade-crippling-cyber-attack-china-2025-2
[21] Autonomy Has Outpaced International Space Law – War on the Rocks
https://warontherocks.com/2025/03/autonomy-has-outpaced-international-space-law/
[22] Create a Global Code of Conduct for Outer Space | Chatham House – International Affairs Think Tank
https://www.chathamhouse.org/2019/06/create-global-code-conduct-outer-space
[23] Section 66F
https://sherloc.unodc.org/cld/fr/legislation/ind/the_information_technology_act_2000/chapter_xi/section_66f/section_66f.html

personal and sensitive data, reflecting a focus on data sovereignty and security[24]. While the DPDP Act is primarily a privacy law, it signals India's intent to regulate digital risks comprehensively.

In the space realm, India's draft Space Activities Bill (2017) (soon to be reintroduced) would create a licensing regime for private space operators, imposing obligations on licensees to avoid harm and insure liabilities[25]. The draft bill, once enacted, is expected to fill a crucial regulatory gap by authorizing and monitoring non-governmental space activities. The Government has already set up IN-SPACe (Indian National Space Promotion and Authorisation Centre) as a one-stop regulator for private space ventures. Under India's new Space Policy (2023), space entities must ensure safe, sustainable operations, and share debris mitigation practices[26]. The policy also envisages greater collaboration and data-sharing to enhance space situational awareness and cybersecurity.

On data protection and cybersecurity, India's approach has also strengthened besides DPDP, India's IT Act empowers the Government to issue cyber security directions (Section 70A) and block offending websites systems (Section 69A) when national security is at stake. The National Cyber Security Coordinator (NCSC) in the PM's office oversees defense against cyberattacks, including on space assets, while CERT-In (the national CSIRT) monitors incidents. Though India lacks a dedicated "cyber warfare law," its existing statutes can be applied to malicious acts (e.g. unauthorized intrusion or denial-of-service attacks on satellites). In sum, India is building a domestic legal toolkit to deter space cyberattacks through criminal penalties and regulatory oversight, even as the international law catches up.

India on the International Stage

India has also leveraged international fora to shape space norms. As G20 president (2023), India hosted a Space Economy Leaders Meeting (SELM) emphasizing "Economy, Responsibility, Alliance" and proposed a "G20 Satellite Mission" on climate and

[24] Understanding India's New Data Protection Law | Carnegie Endowment for International Peace https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en
[25] Comparisons | Global Practice Guides | Chambers and Partners https://practiceguides.chambers.com/practice-guides/comparison/1223/13639/21691-21692-21693-21694-21695-21696-21697
[26] unoosa.org https://www.unoosa.org/documents/pdf/copuos/2023/Statements/31_PM/5_India_31_May_PM.pdf

environment[27]. This agenda highlighted space as a global commons requiring cooperative governance. Within the UN Committee on the Peaceful Uses of Outer Space (COPUOS), India has been a leading voice on long-term sustainability and transparency. At COPUOS in 2023–24, Indian delegates reaffirmed that all space activities must comply with existing laws, guidelines and debris mitigation rules. India has actively supported Transparency and Confidence Building Measures (TCBMs) and called for "legally binding measures" alongside voluntary ones to ensure peaceful space use. Notably, India's 2023 COPUOS statement stressed that national space policy (2023) will create a framework ensuring safe operations and compliance with international norms[28]. Through COPUOS, India also participates in discussions on cyber security and arms control in space.

Beyond the UN, India co-founded the Global Partnership on Artificial Intelligence (GPAI) in 2020, committing to "responsible and human-centric AI" development[29]. While GPAI is broad, its emphasis on AI ethics and security dovetails with concerns about AI in space systems. Moreover, India collaborates bilaterally on space security (e.g. with the US on military-civil space data sharing)[30]. In multilateral disarmament talks (UN Conference on Disarmament), India has traditionally sought to negotiate a ban on weaponizing space. It consistently votes for non-placement-of-weapons resolutions. In 2023 COPUOS, India underlined that "outer space should be used for peaceful purposes" and urged compliance with international treaties[31]. In sum, India is positioning itself both as a rule-taker (adhering to OST/Liability) and a rule-shaper (pushing for norms on sustainability, TCBMs, and AI ethics).

Proposals: ODR, Codes of Conduct, and a "Space Geneva"

To address the legal vacuum, experts propose several innovations. One idea is to establish an Online Dispute Resolution (ODR) mechanism for space incidents. ODR platforms – now widely used in e-commerce and international arbitration allow rapid, tech-enabled resolution

[27] unoosa.org
https://www.unoosa.org/documents/pdf/copuos/2024/statements/5_India.pdf
[28] unoosa.org
https://www.unoosa.org/documents/pdf/copuos/2023/Statements/31_PM/5_India_31_May_PM.pdf
[29] India joins Global Partnership on Artificial Intelligence (GPAI) as a founding member to support the responsible and human-centric development and use of AI
https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1631676
[30] U.S.-India Joint Statement Highlights Space Cooperation
https://space.commerce.gov/u-s-india-joint-statement-highlights-space-cooperation/
[31] unoosa.org
https://www.unoosa.org/documents/pdf/copuos/2023/Statements/31_PM/5_India_31_May_PM.pdf

across borders. For space, an ODR forum (hosted by the UN or space agencies) could let states and companies quickly arbitrate claims of cyber-interference or collisions, avoiding protracted court battles. ODR's strengths borderless access, integrated document exchange, use of AI tools for fact-finding suit the global, technical nature of space disputes[32]. In fact, arbitration experts note that space law currently lacks any binding dispute forum, leaving injured parties to climb sovereign immunity hurdles[33]. A space-specific ODR "space court" or arbitral center could fill this gap, akin to the 1984 ILA Draft Convention on Space Disputes.

Another key proposal is a code of conduct for responsible behavior of AI and military systems in orbit. As Patricia Lewis and others argue, international guidelines (rules of the road) should explicitly govern cyber and autonomous actions in space. For example, satellites might be required to broadcast anonymized "handshakes" or status beacons, enabling other actors to recognize an autonomous maneuver in progress. Nations could agree norms against deceptive practices like false orbit broadcasts or disruptive jamming of emergency channels. Chatham House analysts call for norms addressing "cleaning up debris, principle of non-interference, and how close satellites can manoeuvre"[34]. Extending that, a "Code for AI in Orbit" could ban lethal autonomous conduct: e.g. programming satellites to disable others, or autonomous cyber-satellites designed for sabotage. These rules could be voluntary at first but gain force via universal uptake.

A bold idea some commentators float is a "Space Geneva Convention." This would analogize humanitarian law's protections to the space domain. Although not yet formalized, the notion underscores that attacks on civilian infrastructure from space should be constrained. The ICRC reminds us that even today, Geneva Conventions and the UN Charter apply to space wars: attacking satellites supporting civilian services (like power grids, hospitals, internet) risks civilian harm[35]. A Space Geneva Convention could codify protections – for instance, outlawing strikes on purely civilian satellites, or requiring warning before engaging multi-use

[32] How Online Dispute Resolution Platforms Transform Arbitration - Transnational Matters
https://www.transnationalmatters.com/how-online-dispute-resolution-platforms-transform-arbitration/
[33] Looking Back While Looking Up: A Review of Space Arbitration Topics - Kluwer Arbitration Blog
https://arbitrationblog.kluwerarbitration.com/2023/02/22/looking-back-while-looking-up-a-review-of-space-arbitration-topics/
[34] Create a Global Code of Conduct for Outer Space | Chatham House – International Affairs Think Tank
https://www.chathamhouse.org/2019/06/create-global-code-conduct-outer-space
[35] War, law and outer space reducing human cost of space operations
https://blogs.icrc.org/law-and-policy/2023/08/15/war-law-outer-space-reduce-human-cost-of-military-space-operations/

constellations. While speculative, such a treaty would establish clear red lines, just as the original Geneva Conventions did for land war. Indeed, critics observe there are currently no international rules to govern cyber activity at all; [36]a dedicated space IHL instrument could fill this gap. At minimum, incorporating outer-space scenarios into the existing law-of-war frameworks (as Tallinn Manual 2.0 begins to do) would align space warfare with humanitarian principles.

Conclusion

Outer space is no longer immune to the digital and AI revolutions. As state and non-state actors develop ever more capable cyber and autonomous capabilities, space assets – once regarded as static observers become fronts in the information battlefield. The 1960s' space law regime, embodied in the Outer Space Treaty and related conventions, offers only blunt tools for these nuanced threats. Launching states can be held liable for downed satellites, but no one is currently accountable for a satellite hijacked by remote code. Autonomous satellites can dodge missiles, but also slip through the cracks of "human in command" paradigms. In this context, robust new norms are essential. India, increasingly both a space power and a technology hub, is advancing domestic cybersecurity law and championing international dialog on space security. Its recent legal reforms (such as the IT Act's cyber-terrorism provisions and the new DPDP privacy law) and leadership in forums (G20 space initiatives, COPUOS working groups, AI partnerships) signal an awareness that global space governance is a strategic priority. Looking ahead, creative solutions are needed: digital dispute-resolution platforms can provide flexible arbitration for cross-border incidents; multilateral codes of conduct can set consensual boundaries on AI behavior in orbit; and even a "Space Geneva Convention" may be imagined to protect civilian space assets. By combining national action with imaginative international lawmaking, the world can work to ensure that the final frontier remains a zone of peace and predictability – even as its systems become ever smarter and more connected.

[36] Create a Global Code of Conduct for Outer Space | Chatham House – International Affairs Think Tank
https://www.chathamhouse.org/2019/06/create-global-code-conduct-outer-space