Peer Reviewed

Volume 7
Issue I

ISSN 2582-0311 (Print)
ISSN 2582-0303 (Online)

August 2025

VIPS STUDENT LAW REVIEW

VIVEKANANDA INSTITUTE OF PROFESSIONAL STUDIES - TECHNICAL CAMPUS

Affiliated to GGSIP University, Delhi
Grade A++ Accredited Institution by NAAC & Recognized by Bar Council of India and AICTE,
Recognized under section 2 (f) by UGC, NBA Accredited for MCA Programme
An ISO 9001:2015 Certified Institution

Volume 7, Issue I August, 2025 ISSN 2582-0311 (Print)
ISSN 2582-0303 (Online)

TABLE OF CONTENTS

S. No.	Title of the Paper / Author	Page No.
1.	Sextortion: Addressing the Impact and Law in India *Dr. Smita Sarmah & Dr. Kasturi Gakul*	1
2.	Cyber Operations Against Space Assets: A Legal Reassessment under the Law of Armed Conflict and International Telecommunication Regulation *Raghavendra S Kollurkar*	17
3.	The Basic Structure Doctrine as a Thin Line of Distinction Between Constitutional Amendment & Constitutional Dismemberment: An Analysis *Raajdwip Vardhan & Susmit Isfaq*	28
4.	Faith and Law at Crossroads: Unravelling the Complexities of Cult Crimes in India's Socio-Legal Framework *Saumya Tripathi*	46
5.	Navigating The Extent of Judicial Intervention in Pre-Arbitral Proceedings vis-a-vis Contemporary Judicial Trends in India *Meher Malik*	58
6.	Bridging Arbitration and Mediation: Evaluating the Arb-Med-Arb Hybrid in India's Investor-State Disputes *Jagyansh Kumar*	76
7.	Navigating Conflicts between IBC and PMLA: Prioritizing Insolvency Resolution over Asset Attachment *Shraddha Tiwari*	93
8.	Unearthing the Vices in Presumed Consent Law In Light of Recent Amendments To Transplantation of Human Organs and Tissues Act *Rishi Khemnani & Hardik Jain*	105
9.	Clickwrap Agreement: Validity, Enforceability And Challenges *Akarsh Raj*	115

10. Ethics v. Governance: A Critical Study of Misleading Advertisements And Consumer Rights in India
Palak Sharma 126

11. Post-Decisional Hearing In Administrative Law: Balancing Procedural Fairness And Administrative Efficiency
Garima Bansal 146

12. Balancing Corporate Tax Incentives and Revenue Collection: A Framework for Promoting Sustainable Business Practices in India
Shrey Bhatnagar & Mahi Singh 165

13. Electoral Disqualification Due To Criminal Antecedents: A Comparative Study
Diya Dhall & Suhani Anand 179

14. From Boardrooms to Ecosystems: A Study of Directors' Duty under Section 166(2) and Environmental Concerns With Reference To UK And Indian Laws
Prabhav Tripathi & Gargi Bindal 200

15. The Enforcement Dilemma of Interim Measures in Foreign Seated Arbitration: Emergency Arbitrator's Award in India
Divyam Desai & Shravin Relan 216

LEGISLATIVE COMMENT

16. Legislative Comment on the WAKF (AMENDMENT) BILL, 2025: Quoting the Contemporary Analysis of the Bill
Taarini Bhardwaj 226

Submission Guidelines 234

CYBER OPERATIONS AGAINST SPACE ASSETS: A LEGAL REASSESSMENT UNDER THE LAW OF ARMED CONFLICT AND INTERNATIONAL TELECOMMUNICATION REGULATION

Raghavendra S Kollurkar*

VIPS Student Law Review
August 2025, Vol. 7, Issue 1, 17-27
ISSN 2582-0311 (Print)
ISSN 2582-0303 (Online)
© Vivekananda Institute of Professional Studies
https://vslls.vips.edu/vslr/

ABSTRACT

The militarization of outer space and the increasing reliance on satellite constellations for civilian and military functions have introduced complex legal challenges under the evolving landscape of cyber warfare. This research article critically examines the legality of cyber-attacks targeting space assets, particularly satellite constellations, under the Law of Armed Conflict (LOAC) and International Telecommunication Union (ITU) regulations. By exploring the dual-use nature of satellites, the principle of distinction, and the thresholds for lawful targeting and proportionality, the research article reveals significant ambiguities in applying traditional LOAC principles to cyber operations in space. It further interrogates the role of ITU frameworks in safeguarding spectrum integrity and satellite operations during armed conflict. Through an integrated analysis of international legal norms, state practice, and emerging doctrines, the research article advocates for a nuanced reassessment of existing regulatory regimes. It calls for the development of tailored legal standards to address the vulnerabilities of space assets to cyber threats while preserving the stability and sustainability of outer space as a global common. In doing so, it contributes to the urgent discourse on adapting international law to the realities of modern conflict in the cyber and space domains.

Keywords: *Cyber Operations, Armed Conflict, Telecommunication Regulation, International Law, Cyber Warfare*

* Assistant Professor, (JRF Scholar), Adv. P. C. Patil Law College
Email ID: raghavkollurkar@gmail.com.

1. INTRODUCTION

In February 2022, amidst the unfolding Russia-Ukraine conflict, a cyberattack targeted Viasat's KA-SAT satellite network, disrupting broadband internet services across Europe, including affecting critical infrastructure and civilian communications in Ukraine.[1] This incident starkly highlighted the growing vulnerabilities of space-based assets to cyber operations and foreshadowed the emerging reality where outer space is a contested domain in modern warfare.

The increasing reliance on satellite constellations for communications, navigation, intelligence, and military operations has rendered space infrastructure a strategic asset and, consequently, a lucrative target.[2] This militarization of space, coupled with rapid technological advancements, has introduced unprecedented cybersecurity risks.[3] Satellites, traditionally viewed as remote and resilient, are now susceptible to sophisticated cyberattacks capable of causing widespread disruption without physical destruction.

Despite the growing threat landscape, there remains a significant lacuna in the international legal framework governing cyberattacks on space assets.[4] While the Law of Armed Conflict (LOAC) provides foundational principles such as distinction and proportionality, its application to cyber operations in outer space is ambiguous and lacks specificity.[5] Similarly, the International Telecommunication Union (ITU) regulations primarily address spectrum management and technical coordination but offer limited mechanisms to prevent or respond to malicious cyber activities targeting satellites.[6]

This article critically examines the legality of disabling satellite constellations through cyber means under LOAC and ITU regulations. It identifies key legal gaps and ambiguities, analyzes recent incidents and evolving threats, and proposes concrete reforms to enhance the resilience and protection of space assets in contemporary armed conflicts.

1 Viasat Inc., *Viasat Shares Update on Cyberattack Affecting KA-SAT Network in Europe,* (2022), https://news.viasat.com/news/news-releases/viasat-shares-update-on-cyberattack-affecting-ka-sat-network-in-europe.

2 United Nations Office for Outer Space Affairs, *Space Solutions for the World's Problems* (2021), https://www.unoosa.org/oosa/en/space-sdg/index.html.

3 Secure World Foundation, *Global Counterspace Capabilities: An Open Source Assessment* (2023), https://swfound.org/reports/global-counterspace-capabilities-2023.

4 David Turns, *Cyber Operations and the Law of Armed Conflict*, 91 Int'l L. Stud. 218, 220 (2015).

5 Michael N. Schmitt, ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 114–19 (2d ed. 2017).

6 Int'l Telecomm. Union, Constitution and Convention of the International Telecommunication Union, art. 45 (2019).

2. THE STRATEGIC IMPORTANCE OF SATELLITE CONSTELLATIONS

Satellite constellations have become indispensable to modern society and military operations. Their critical functions include providing global communications, enabling precision navigation through systems like the Global Positioning System (GPS), supporting intelligence, surveillance, and reconnaissance (ISR) capabilities, and facilitating military targeting and command-and-control operations.[7] The seamless integration of space-based assets into terrestrial and military infrastructures underscores their strategic significance in both peacetime and armed conflict.[8]

However, as reliance on satellites grows, so too do their vulnerabilities. Satellites and their ground stations are susceptible to a range of threats, including jamming, which disrupts signals; spoofing, which manipulates navigation data; malware infiltration of satellite control systems; and kinetic attacks such as anti-satellite (ASAT) missile strikes.[9] These vulnerabilities expose space infrastructure to potential disruptions that can cascade across civilian and military domains, highlighting the urgent need for enhanced security measures.

The landscape of space actors has also shifted dramatically. No longer dominated solely by state actors, the domain now includes prominent private companies such as SpaceX, Amazon, and OneWeb.[10] SpaceX's Starlink constellation, for instance, has played a crucial role in maintaining internet connectivity in conflict zones, while Amazon's Project Kuiper and OneWeb aim to provide global broadband coverage.[11] This privatization and commercialization of space assets blur traditional distinctions between civilian and military targets under international law, raising complex legal and operational challenges.[12] The involvement of private actors in space operations necessitates a reassessment of existing legal frameworks to address issues of attribution, accountability, and the protection of critical infrastructure during armed conflict.

7 Brian Weeden & Victoria Samson, *Global Counterspace Capabilities: An Open Source Assessment,* 1 SECURE WORLD FOUNDATION (2023).

8 U.S. Dep't of Def., *Defense Space Strategy Summary* 3–5 (2020), https://media.defense.gov/2020/Jun/17/2002317391/-1/-1/1/DEFENSE-SPACE-STRATEGY-SUMMARY-JUNE-2020.PDF.

9 Aaron Bateman, *Why Space is the Next Frontier for Cybersecurity,* FOREIGN POL'Y (Apr. 5, 2022), https://foreignpolicy.com/2022/04/05/space-cybersecurity-satellites-vulnerabilities/.

10 SECURE WORLD FOUNDATION, SWF HANDBOOK FOR NEW ACTORS IN SPACE 4–6 (2d ed. 2020).

11 Mike Wall, *SpaceX's Starlink Satellite Internet for Ukraine Shows the Promise and Peril of Mega-Constellations*, SPACE.COM (Mar. 21, 2022), https://www.space.com/spacex-starlink-ukraine-communications.

12 Jack Beard, *Soft Law's Failure on the Horizon: The International Code of Conduct for Outer Space Activities*, 38 U. PA. J. INT'L L. 335, 375–78 (2017).

3. LEGAL FRAMEWORK GOVERNING CYBER OPERATIONS IN SPACE

Cyber operations targeting space assets operate in a complex legal environment where existing frameworks are often stretched to their limits. Traditional instruments such as the Outer Space Treaty (OST) of 1967, the Geneva Conventions, and the United Nations Charter provide foundational norms but were not designed to address the unique challenges posed by cyberattacks on satellite constellations.[13]

The Outer Space Treaty prohibits the placement of weapons of mass destruction in orbit and mandates the peaceful use of outer space.[14] However, it remains silent on non-kinetic cyber operations that can disable or disrupt satellites without physical damage.[15] Additionally, Article VI of the OST imposes state responsibility for national activities in outer space, whether conducted by governmental or non-governmental entities, thus extending obligations to private actors like SpaceX and OneWeb.[16] Yet, the treaty offers limited guidance on how liability and accountability should be assessed in cases of cyber interference.

Under the Law of Armed Conflict (LOAC), principles such as distinction, proportionality, and necessity govern the conduct of hostilities, including in the cyber domain.[17] Military satellites that contribute directly to military operations could be considered lawful targets under LOAC, while civilian satellites retain protections unless they are used for military purposes.[18] However, dual-use satellites those serving both civilian and military functions complicate the application of LOAC principles, raising concerns about the proportionality and collateral damage of cyber operations.[19]

The International Telecommunication Union (ITU) Regulations, particularly the Constitution and the Radio Regulations, seek to ensure the equitable and interference-free use of the

13 Setsuko Aoki, *Space Law and Space Security: The Role of International Space Law*, 44 J. Space L. 25, 30–33 (2020).

14 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies art. IV, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 [hereinafter Outer Space Treaty].

15 Steven Freeland, Cyber Operations and the "Peaceful Uses" of Outer Space, in The Oxford Handbook of the Law of Armed Conflict 790, 794 (Andrew Clapham et al. eds., 2015).

16 Outer Space Treaty, *supra* note 2, art. VI.

17 Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 347–48 (ed., 2017).

18 Michael N. Schmitt, *Wired Warfare: Computer Network Attack and the Jus in Bello*, 84 Int'l Rev. Red Cross 365, 379 (2002).

19 Wolff Heintschel von Heinegg, *The Law of Armed Conflict and the Protection of Space Objects from Hostilities*, 55 German Y.B. Int'l L. 118, 126–28 (2012).

radio-frequency spectrum and satellite orbits.[20] The ITU prohibits harmful interference with radio communications but lacks robust enforcement mechanisms, especially in cases where interference is intentional and linked to armed conflict.[21] Moreover, the ITU framework does not adequately address state responsibility for cyber disruptions, leaving a critical regulatory gap.

In sum, while existing legal instruments provide a partial framework, significant ambiguities persist regarding the legality of cyber operations against space assets. The evolving nature of space technology and the growing militarization of the domain demand a reassessment of these legal norms to ensure the protection of critical infrastructure in times of both peace and conflict.

4. CASE STUDIES OF CYBER OPERATIONS TARGETING SATELLITES

Real-world incidents reveal the growing threat landscape for space-based assets, particularly through cyber means. These case studies highlight vulnerabilities and expose the inadequacy of current legal frameworks.

4.1 Viasat Hack during Russia-Ukraine Conflict (2022)

In February 2022, a cyberattack targeted Viasat's KA-SAT satellite network, resulting in widespread disruption of broadband services across Ukraine and parts of Europe.[22] The attack, attributed to Russian state actors by Western governments, disabled thousands of modems through a malicious firmware update.[23] Although primarily affecting civilian infrastructure, the attack indirectly hampered Ukrainian military communications, illustrating the blurred lines between civilian and military uses of satellite networks.[24] Notably, no physical damage occurred, complicating the classification of the attack under existing LOAC principles.

20 Constitution of the International Telecommunication Union, Dec. 22, 1992, 1825 U.N.T.S. 3, art. 45; International Telecommunication Union, Radio Regulations (2020 ed.).

21 Fabio Tronchetti, *The ITU and the Protection of Satellites: Problems and Prospects*, 36 J. Space L. 41, 49–50 (2010).

22 U.S. Dep't of State, *Russia's Global Cyber Influence: Hacking Viasat in Ukraine* (Mar. 2022), https://www.state.gov/russias-global-cyber-influence-hacking-viasat-in-ukraine.

23 European Union, Council Decision 2022/1507, Restrictive Measures Against Cyberattacks Threatening the Union or Its Member States (Sept. 9, 2022).

24 Kristen Eichensehr, *The Viasat Cyberattack and the Law of War*, Just Security (Mar. 2022), https://www.justsecurity.org/80819/the-viasat-cyberattack-and-the-law-of-war/.

The Viasat incident raises key questions: Can disabling satellites through non-destructive means constitute an "attack" under international law? What protections should dual-use assets receive? These ambiguities highlight the urgent need for doctrinal clarity.

4.2 Alleged Chinese Cyber Espionage on U.S. Satellites

Reports indicate that between 2007 and 2008, U.S. government satellites, including Landsat-7 and Terra AM-1, experienced repeated interference allegedly originating from China.[25] Hackers reportedly gained control over satellite operations via a ground station in Norway.[26] Although no permanent damage occurred, the intrusions demonstrated the potential for cyber operations to seize command and control of critical space infrastructure without kinetic force.[27]

This episode underscores the loopholes in current space and cyber norms: hostile intrusions that fall below the threshold of an armed attack remain largely unregulated.

4.3 Iran's Jamming of Satellite Broadcasts

Iran has been repeatedly accused of jamming satellite transmissions, particularly foreign news broadcasts.[28] In 2012, the ITU officially warned Iran for deliberate interference with satellite signals in violation of the Radio Regulations.[29] Although the jamming was electromagnetic rather than cyber-based, the incident illustrates the broader vulnerabilities of satellite systems to hostile actions and the limited enforcement power of international organizations.

5. LEGAL ANALYSIS: APPLICATION OF LOAC AND ITU RULES TO CYBER OPERATIONS AGAINST SPACE ASSETS

5.1 Threshold of an *"Attack"* Under the Law of Armed Conflict (LOAC)

Under LOAC, an *"attack"* is defined as *"acts of violence against the adversary, whether in*

25 U.S.-China Econ. & Sec. Rev. Comm'n, *2011 Report to Congress* 243–45 (Nov. 2011).

26 William J. Lynn III, *Defending a New Domain: The Pentagon's Cyberstrategy*, 89 Foreign Aff. 97, 103 (2010).

27 David E. Sanger & William J. Broad, *From a Chinese Base, Hacking U.S. Satellites,* N.Y. Times (Oct. 28, 2011), https://www.nytimes.com/2011/10/28/world/asia/satellite-hacks-point-to-chinas-growing-pains.html.

28 Int'l Telecomm. Union (ITU), Report on Harmful Interference to Satellite Services in Iran (2012).

29 *Id.*

offense or in defense."[30] Traditionally, this presupposes kinetic harm. However, in cyber operations, the absence of physical destruction complicates qualification as an *"attack"*[31] The Tallinn Manual 2.0 suggests that cyber operations causing loss of functionality may qualify as attacks if the effects are comparable to those of kinetic force.[32]

Applying this logic to satellite cyberattacks such as the Viasat incident the disabling of operational capabilities could meet the threshold of an "attack," especially if it disrupts critical civilian or military services.[33] Nonetheless, divergent interpretations among states persist, creating uncertainty regarding lawful responses.

5.2 Principles of Distinction and Proportionality

LOAC requires parties to a conflict to distinguish between civilian objects and military objectives.[34] Satellites, particularly those operated by private corporations like SpaceX or OneWeb, often serve both civilian and military functions.[35] The principle of dual-use complicates their legal status: while a satellite transmitting military data may become a lawful target, collateral damage to its civilian functions must be proportionate to the anticipated military advantage.[36]

In cyber operations, unintended spillover effects such as harming civilian internet services while targeting military communications pose heightened risks of violating proportionality obligations.[37] States must thus exercise heightened diligence in planning cyberattacks on space infrastructure.

30 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 49(1), June 8, 1977, 1125 U.N.T.S. 3.

31 Michael N. Schmitt, *Wired Warfare: Computer Network Attack and the Jus in Bello*, 84 Int'l Rev. Red Cross 365, 372–73 (2002).

32 Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations R. 92 CMT. 6 (2d ed. 2017).

33 Kristen Eichensehr, *The Viasat Cyberattack and the Law of War*, Just Security (Mar. 2022), https://www.justsecurity.org/80819/the-viasat-cyberattack-and-the-law-of-war/.

34 Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War art. 48, Aug. 12, 1949, 75 U.N.T.S. 287.

35 Kaitlyn Johnson, *SpaceX and the Dual-Use Dilemma of Commercial Satellites*, Ctr. for Strategic & Int'l Stud. (Feb. 2022), https://www.csis.org/analysis/spacex-and-dual-use-dilemma-commercial-satellites.

36 Yoram Dinstein, The Conduct of Hostilities Under the Law of International Armed Conflict 88 (3d ed. 2016).

37 Michael Schmitt & Liis Vihul, *Proxy Wars in Cyber Space: The Evolving International Law Framework*, 49 Geo. J. Int'l L. 1227, 1244–45 (2018).

5.3 ITU Regulations and the Principle of Non-Interference

The International Telecommunication Union (ITU) Constitution mandates the non-interference with radio services and the rational use of the radio-frequency spectrum.[38] Under Article 45, Member States must "refrain from causing harmful interference to the radio services of other Member States."[39]

Cyber operations targeting satellites that cause jamming, signal manipulation, or hacking can breach ITU obligations. However, the ITU lacks enforcement mechanisms akin to the United Nations Security Council, limiting its practical deterrence value.[40] Further, the ITU framework was not designed to address hostile acts during armed conflicts, creating a normative vacuum when cyber hostilities involve space assets.

5.4 Attribution Challenges

Attributing cyberattacks to a specific state actor is notoriously difficult.[41] The Viasat hack, despite strong suspicions against Russia, lacked immediate public technical attribution.[42] Under LOAC, proper attribution is crucial for holding states accountable and invoking lawful countermeasures or self-defense.[43] Space assets, with their reliance on globally distributed infrastructure, exacerbate these attribution challenges, underscoring the urgent need for enhanced technical standards and political consensus on attribution thresholds.

5.5 Gaps and Ambiguities

Both LOAC and ITU rules exhibit significant gaps when applied to cyber operations against satellites:

a. Threshold Uncertainty: Lack of consensus on when a cyber operation constitutes an "attack."

b. Dual-Use Dilemmas: Difficulties in distinguishing lawful targets from civilian objects.

38 Constitution of the International Telecommunication Union, Dec. 22, 1992, 1825 U.N.T.S. 3 (hereinafter ITU Constitution).

39 ITU Const. art. 45.

40 Fabio Tronchetti, *The ITU Framework and Space Security: Assessing the Limits*, 45 J. Space L. 163, 179–81 (2019).

41 U.S. Cyberspace Solarium Comm'n, Final Report 43–46 (Mar. 2020).

42 European Union, Council Decision 2022/1507, Restrictive Measures Against Cyberattacks Threatening the Union or Its Member States (Sept. 9, 2022).

43 Tallinn Manual 2.0, *supra* note 3, r. 15.

c. Weak Enforcement: Absence of robust mechanisms in ITU regulations.

d. Attribution Problems: Hurdles in proving state responsibility.

These gaps suggest the need for doctrinal development, either through new international treaties, interpretive guidance, or state practice crystallizing into customary law.

6. SUGGESTIONS FOR STRENGTHENING INTERNATIONAL LEGAL PROTECTIONS

6.1 Codify Cyber Operations Against Space Assets in a New Treaty

The existing legal frameworks LOAC, the Outer Space Treaty, and ITU regulations were not designed with cyber warfare in mind. A specialized treaty addressing cyber operations against space infrastructure should be negotiated under United Nations auspices.[44] This instrument should define prohibited conduct, clarify the threshold for *"attacks,"* and establish mandatory transparency and notification obligations.

Such a treaty could draw inspiration from the Geneva Conventions' protection of civilians and the Tallinn Manual's cyber norms, explicitly extending protections to dual-use commercial satellites essential for civilian life.[45]

6.2 Develop Interpretive Guidance for Existing LOAC Norms

Pending treaty development, states should adopt interpretive guidance similar to the San Remo Manual for naval warfare applying LOAC principles to cyber operations in space.[46] This guidance should clarify:

a. When a cyber operation against a satellite constitutes an *"attack."*

b. How the principles of distinction and proportionality apply to dual-use systems.

c. The obligation to minimize harm to civilian space assets.

Such clarity would reduce legal ambiguity and enhance compliance during armed conflicts involving space systems.

44 U.N. Office for Outer Space Affairs, *Space2030 Agenda: Space as a Driver of Sustainable Development* (2021), https://www.unoosa.org/oosa/en/ourwork/space2030/index.html.

45 TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS R. 92 CMT. 6 (MICHAEL N. SCHMITT ed., 2d ed. 2017).

46 Int'l Inst. of Humanitarian L., *San Remo Manual on International Law Applicable to Armed Conflicts at Sea* (1994).

6.3 Strengthen Attribution Mechanisms

Effective attribution remains a linchpin for accountability.[47] States should invest in technical capabilities for satellite cybersecurity forensics and support multilateral initiatives like the Paris Call for Trust and Security in Cyberspace.[48]

Additionally, cooperative frameworks, potentially modeled on the Chemical Weapons Convention's inspection mechanisms, could enable neutral technical fact-finding after cyber incidents affecting space assets.[49]

6.4 Enhance ITU Enforcement and Update Regulations

The ITU should reform its procedures to better address cyber interference with satellite communications.[50] Possible measures include:

a. Establishing a cyber incident reporting mechanism within the ITU.

b. Creating a technical advisory board for cyber threats to the radio spectrum.

c. Promoting binding dispute resolution for harmful interference claims.

Modernizing ITU regulations would deter malicious state behavior and better protect critical satellite functions.

6.5 Promote Norms of Responsible Behavior in Outer Space

States should endorse and operationalize the norms proposed by the UN Group of Governmental Experts (GGE) on responsible behavior in cyberspace, particularly those related to critical infrastructure protection.[51]

Expanding these norms to specifically reference space-based infrastructure would reinforce the principle that satellites indispensable for civilian life should be off-limits during peacetime and conflict alike.[52]

47 Kristen Eichensehr, *The Law & Politics of Cyberattack Attribution*, 67 UCLA L. Rev. 520, 540–42 (2020).

48 Paris Call for Trust and Security in Cyberspace, (Nov. 12, 2018) https://pariscall.international/.

49 Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction art. IX, Jan. 13, 1993, 1974 U.N.T.S. 45.

50 Fabio Tronchetti, *The ITU Framework and Space Security: Assessing the Limits*, 45 J. Space L. 163, 179–81 (2019).

51 U.N. Group of Governmental Experts, Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98 (June 24, 2013).

52 *Id.*

7. CONCLUSION

The cyberattack on Viasat during the early stages of the Russia-Ukraine conflict[53] exposed a critical truth: space assets are no longer immune from the turbulence of terrestrial warfare. As militaries increasingly rely on satellite constellations for communications, navigation, surveillance, and targeting,[54] the risk of cyber operations targeting these systems will only intensify.

Yet the legal frameworks governing armed conflict the Outer Space Treaty, LOAC, and ITU regulations were crafted for an era before cyberspace became a domain of warfare.[55] They leave substantial ambiguity regarding what constitutes an "attack" against space assets, the protections afforded to dual-use commercial satellites, and mechanisms for enforcing prohibitions on harmful interference.[56]

This legal vacuum creates dangerous incentives for states to launch cyberattacks under the threshold of kinetic use of force, destabilizing not just military balances but also critical civilian infrastructure worldwide.[57]

Immediate action is imperative. States must urgently work toward negotiating new binding agreements, or at least robust interpretive guidance, to clarify the application of international law to cyber operations against space systems.[58] Attribution capabilities must be enhanced, ITU enforcement mechanisms modernized, and norms of responsible behavior in outer space reinforced.[59]

Space has become an extension of the modern battlefield. Protecting satellites from cyberattacks is not merely a matter of strategic advantage it is essential to safeguarding civilian life, economic stability, and international peace. Inaction risks opening a Pandora's box that humanity may not be able to close.

53 David E. Sanger & Julian E. Barnes, *Russia Hacked an American Satellite Company One Hour Before the Ukraine Invasion*, N.Y. Times (May 10, 2022), https://www.nytimes.com/2022/05/10/us/politics/russia-ukraine-cyberattack.html.

54 National Aeronautics and Space Administration, *The Role of Satellites in Modern Warfare*, NASA Technical Reports (2022).

55 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies arts. III–IV, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 [hereinafter Outer Space Treaty].

56 Michael N. Schmitt, *Conflict in Space: International Humanitarian Law and Its Application to Space Warfare*, 48 Colum. J. Transnat'l L. 1, 27–29 (2009).

57 Kristen Eichensehr, *The Law & Politics of Cyberattack Attribution*, 67 UCLA L. Rev. 520, 540–42 (2020).

58 Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations R. 92 (2d ed. 2017).

59 U.N. Group of Governmental Experts, Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98 (June 24, 2013).