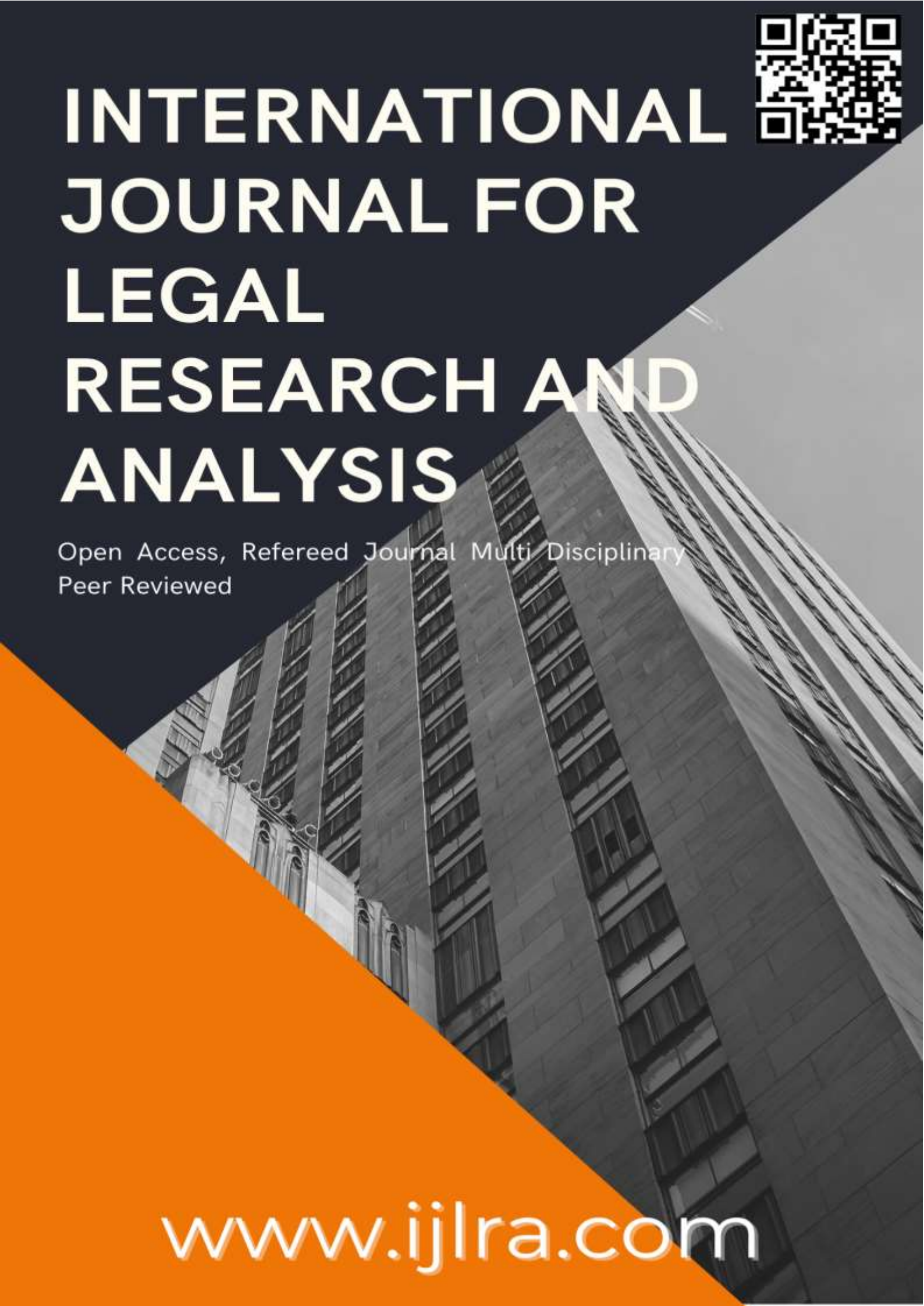
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

SPACE-CYBER LAW: REGULATING COMMERCIAL SATELLITE NETWORKS IN GEOPOLITICAL CONFLICTS

AUTHORED BY - ALOK SINGH

ABBREVIATIONS

AI	Artificial Intelligence
AIR	All India Report
BNS	Bharatiya Nyaya Sanhita,
CISA	Cybersecurity and Infrastructure Security Agency
DPDP	Digital Personal Data Protection
ENISA	European Union Agency for Cybersecurity
ESA	European Space Agency
GDPR	General Data Protection Regulation
GPS	Global Positioning System
IHL	International Humanitarian Law
IT Act	Information Technology Act
NATO	North Atlantic Treaty Organization
OST	Outer Space Treaty
UK	United Kingdom
US	United States
UN	United nation
UOI	Union of India

ISSN: 2582-6433

LIST OF CASES

Anand Chawla v. Union of India, Writ Petition (Criminal) No. 46/2021

Devas Multimedia v. Antrix Corporation Ltd. Civil Appeal Nos. 5766 & 5906 of 2021

United States v. North Korea No. 1:14-cv-08935 (S.D.N.Y. Dec. 18, 2014).

Barreiro et al. v. Alphabet Inc No. 1:20-cv-00242 (D.D.C. Jan. 28, 2022).

Airbus Defence and Space GmbH v. Northrop Grumman Systems Corp No. 1:21-cv-00642 (E.D. Va. 2021).

United States v. Microsoft Corp. 594 U.S. ___ (2021)

Twitter, Inc. v. Taamneh598 U.S. 471 (2023)

Nicaragua v. Germany ICJ Case No: 193.(2024)

Benabderrahmane v. Qatar (2025). Opinion No. 28/2025

United States v. Omer Crim. No. 09-242

ISSN: 2582-6433

TABLE OF CONTENTS

ISSN: 2582-6433

ABSTRACT

The convergence of space-based technologies and cyber operations has transformed modern conflict dynamics. Commercial satellite networks, initially designed for civilian purposes, are increasingly being leveraged for military and strategic operations, particularly in geopolitical hotspots. This dual-use nature raises complex legal, regulatory, and ethical challenges, as private operators may inadvertently or deliberately become entangled in international conflicts. The absence of binding legal frameworks leaves both states and corporations vulnerable to liability and operational risks.

Despite the growing reliance on commercial satellites in warfare and critical infrastructure, existing international and national legal instruments are insufficient to address the unique risks posed by these dual-use systems. Voluntary guidelines and best practices provide limited guidance and lack enforceability, resulting in inconsistencies in security standards, accountability, and operational oversight. Cyberattacks, such as the 2022 KA-SAT disruption, highlight the potential consequences of inadequate regulation, including civilian collateral damage and strategic vulnerabilities.

This study aims to examine the legal and regulatory frameworks governing commercial satellite networks in geopolitical conflicts. It explores the interplay between international space law, cyber law, and corporate responsibility, analyzing case studies where commercial operators played pivotal roles in conflicts. The foundational legal framework governing outer space, chiefly the 1967 Outer Space Treaty, was originally crafted during the Cold War with the primary aim of regulating physical objects and conventional, kinetic forms of warfare, such as missile deployment. At the time, drafters could not have foreseen a future dominated by private companies launching vast constellations of satellites. Moreover, the OST does not address the emergence of non-kinetic cyber weapons capable of disrupting critical infrastructure entirely without causing any physical destruction. The research employs a qualitative, doctrinal approach, integrating legal analysis with case study evaluation. Key incidents, including the KA-SAT cyberattack and Starlink's deployment in Ukraine, are examined to illustrate operational, legal, and ethical challenges. Comparative analysis of international treaties, national regulations, and voluntary guidelines provides insight into regulatory inconsistencies and enforcement limitations. Additionally, corporate governance practices are assessed to understand the accountability mechanisms available to private operators in dual-use contexts.

The study finds that voluntary cybersecurity and operational guidelines are insufficient to

ISSN: 2582-6433

mitigate the risks posed by dual-use satellite networks. Mandatory regulatory frameworks, such as the European Union's security-by-design requirements, provide enforceable standards that integrate cybersecurity throughout the lifecycle of space assets. Case studies demonstrate that legally binding obligations enhance corporate accountability, clarify liability, and reduce vulnerabilities in both civilian and military applications. Furthermore, international cooperation and harmonization of standards are critical for managing the transnational nature of space operations.

Regulating commercial satellite networks in geopolitical conflicts requires a multi-faceted approach that combines enforceable legal standards, corporate governance, and international coordination. By transitioning from voluntary guidance to mandatory regulation, states can ensure baseline security, protect civilian infrastructure, and maintain strategic stability. The findings underscore the need for adaptive legal frameworks capable of addressing emerging technologies, hybrid warfare, and evolving cyber threats. This research contributes to the development of space-cyber law as a critical discipline for managing the risks of dual-use technologies in an increasingly contested global environment.

ISSN: 2582-6433

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND OF THE STUDY

The dramatic growth of commercial satellite constellations has fundamentally altered the character of outer space, shifting it from a domain controlled almost exclusively by governments to one increasingly shaped by private enterprise. Corporations now operate expansive networks that deliver broadband connectivity, Earth observation data, navigation services, and other critical capabilities worldwide. Enterprises such as SpaceX, through its Starlink system, and OneWeb exemplify this transformation. Their infrastructure supports not only civilian life but also national defense functions, embedding commercial space assets within the fabric of modern geopolitics.

The cornerstone of international space governance remains the OST, which articulates major aspects comprising peaceful utilization of outer space, the prevention of national appropriation, and the attribution of responsibility to states for activities conducted under their jurisdiction. Yet this framework was negotiated at a time when space activity was monopolized by sovereign states. The emergence of powerful private satellite operators exposes the limitations of a treaty regime that did not anticipate privately owned mega-constellations with strategic significance.

A defining feature of contemporary satellite networks is their dual-use nature. Commercial systems designed for civilian communications can also facilitate military command, intelligence sharing, and operational coordination. The reliance on commercial connectivity during the Russian invasion of Ukraine demonstrated how integral such services can be to national resilience and defense. This overlap between civilian and military utility complicates their classification under international humanitarian law, especially when assessing whether they constitute legitimate military objectives during armed conflict.[1]

Companies such as SpaceX & Amazon are deploying vast constellations of low Earth orbit satellites, enabling high-speed internet access, precise positioning services, and real-time data collection across the globe. This commercialization has created opportunities for economic growth, scientific research, and technological innovation. Simultaneously, the reliance on satellite-based infrastructure has introduced new vulnerabilities. Satellite signals, including those used for GPS, communications, and remote sensing, can be intercepted, jammed, or

[1] Johnson, D. G., & Wetzel, R. (2020). The cyber-space convergence: Legal and strategic implications of dual-use satellite networks. Journal of Strategic Studies, 43(6), 847–872

ISSN: 2582-6433

manipulated. Threats such as signal spooling, spoofing, and data interception now pose significant risks not only to commercial operations but also to national security and military systems, highlighting the critical intersection between space and cyber domains.

Simultaneously, the convergence of space infrastructure and cyber capabilities has created new vulnerabilities. Cyber operations targeting satellite ground stations, control software, or user terminals can neutralize orbital assets without the need for kinetic force. Disruptions linked to actors targeting networks operated by companies such as Viasat underscore the exposure of commercial systems to hostile cyber activities. These incidents blur the boundaries between cyber interference, prohibited uses of force, and acts that may trigger self-defense rights under international law.

The doctrine of state responsibility further intensifies the regulatory dilemma. Pursuant to Article VI (OST), states remain internationally accountable for space activities carried out by private actors within their jurisdiction. Consequently, the conduct of a commercial satellite provider—whether through active assistance to a belligerent or insufficient cybersecurity safeguards—may implicate the legal responsibility of its home state. The precise threshold at which commercial services amount to direct participation in hostilities remains uncertain and contested.

Neutrality law introduces another layer of complexity. If a private satellite operator furnishes services that materially benefit one side in an armed conflict, questions arise as to whether this affects the neutral status of the state under whose authority the company operates. Traditional neutrality doctrines were formulated with physical supplies and troop movements in mind, not digital data streams transmitted globally from space. Applying geographically rooted neutrality rules to borderless satellite services poses significant interpretative challenges.

Moreover, regulatory inconsistencies among states exacerbate the problem. Domestic licensing frameworks differ substantially in their treatment of cybersecurity standards, spectrum management, and export restrictions. While institutions such as the International Telecommunication Union coordinate technical matters like orbital slot allocation and radiofrequency usage, they do not possess robust mechanisms to police conduct during geopolitical crises. This patchwork governance environment risks leaving commercial constellations inadequately protected and insufficiently regulated.[2]

[2] Kremer, J., & Mueller, M. (2019). Cyber-attacks, dual-use space systems, and international humanitarian law: Legal gaps and emerging frameworks. Journal of Space Law, 43(1), 55–88.

ISSN: 2582-6433

Regarding this development, the governance of commercial satellite networks amid geopolitical conflict demands a more coherent and integrated legal response. Space-cyber law must bridge the gap between longstanding principles embedded in the Outer Space Treaty and the contemporary realities of privatized, dual-use, and cyber-dependent infrastructure. As commercial constellations become ever more central to global communications and security, clarifying their legal status and obligations will be critical to safeguarding both international stability and the sustainable use of outer space.[3]

In the Indian context, the rapid expansion of satellite-based internet services and the strategic deployment of dual-use space infrastructure has highlighted the urgent need for legal and regulatory clarity. India's commercial satellite sector, led by private operators and public-private partnerships, is increasingly intertwined with national security objectives. Cases such as Devas Multimedia v. Antrix Corporation Ltd.[4] and regulatory scrutiny over spectrum allocation illustrate the interplay between commercial ambitions, state oversight, and legal accountability. Meanwhile, India's policy initiatives, including the National Space Policy 2023 and the Indian Cyber Security Guidelines, reflect efforts to address cybersecurity, data protection, and strategic vulnerability, but gaps remain in governing dual-use satellite networks in conflict scenarios.

From a legal perspective, the Indian experience underscores the limitations of traditional space law and cyber law when applied to emerging commercial satellite networks. The Outer Space Treaty and related instruments, although ratified by India, were drafted in a state-dominated, Cold War era and do not sufficiently cover private operators or non-kinetic cyber threats. Similarly, Indian cyber and privacy jurisprudence, including the K.S. Puttaswamy[5] judgment on the right to privacy and Anand Chawla v. Union of India[6]on intermediary obligations, provides some guidance but requires adaptation for space-based networks. This creates a pressing need to develop integrated legal frameworks that address commercial satellite regulation, cybersecurity responsibilities, and national security imperatives while aligning with both domestic law and international norms, particularly in the context of geopolitical conflicts where satellite networks are increasingly leveraged as strategic assets.

The evolution of space infrastructure from state-owned monopolies to commercial "mega-

[3] Moltz, J. C. (2019). Space security and cyber interdependencies: Challenges for global governance. Space Policy, 47, 101–110

[4] Civil Appeal Nos. 5766 & 5906 of 2021

[5]KS Puttaswamy v. UOI (2017) 10 SCC 1

[6] Anand Chawla v. Union of India, Writ Petition No. 20008 of 2013

ISSN: 2582-6433

constellations."

I. The Age of State-Controlled Space Systems

The origins of space infrastructure were deeply intertwined with the geopolitical tensions of the Cold War, a period during which outer space was viewed as a critical domain for technological, military, and ideological dominance. In 1958, the United States established NASA to spearhead both scientific exploration and strategic technological development, while the Soviet Space Program had already demonstrated significant capabilities through the launch of Sputnik and subsequent human spaceflights, signaling Soviet leadership in rocketry and orbital deployment. During this era, satellites were designed almost exclusively to serve national objectives, including reconnaissance, missile detection, scientific observation, and early communications. The U.S. Corona program, for example, deployed a series of classified reconnaissance satellites to photograph the Soviet Union, providing intelligence that was otherwise inaccessible through conventional aerial reconnaissance. Similarly, early communications satellites like Telstar and Relay, although eventually integrated into commercial applications, were initially heavily supervised by government authorities and were designed with dual civilian and military objectives in mind. Meteorological satellites, such as the U.S. TIROS series and the Soviet Meteor series, provided critical weather data that informed both agricultural planning and military operations. The defining characteristic of this period was complete state control: governments funded the research, designed the spacecraft, managed the launches, and operated the orbital systems. Private participation was largely limited to subcontracting, and the immense cost and technological complexity of space access ensured that only sovereign states could operate in orbit.[7]

This state-dominated period was reinforced by legal frameworks designed specifically for government actors. The OST formalized the state-centric model, with Article VI stipulating that states must authorize and supervise all national space activities, including those undertaken by private entities, and remain internationally responsible for them. This framework assumed that governments would continue to be the primary operators in space, and that commercial involvement would be minimal and closely regulated. Even today, national licensing regimes reflect this legacy. In the United States, for instance, private satellite operators must secure Federal Communications Commission authorization to use

[7] Moltz, J. C. (2018). The politics of space security: Strategic considerations in state-controlled space systems. Space Policy, 45, 12–21

ISSN: 2582-6433

orbital slots and frequencies, and export controls such as ITAR restrict the transfer of sensitive satellite technologies, maintaining state oversight over what might otherwise be a commercial domain.[8]

Early Commercial Participation

By the late twentieth century, gradual commercialization began reshaping the space sector. Geostationary satellites provided a stable orbital platform with continuous coverage over fixed regions, making them particularly attractive for private communications services. Private companies began deploying satellites to deliver television broadcasting, telephony, and other data services across broad geographic areas. The International Telecommunication Union played a crucial role in this expansion, coordinating orbital slots and radiofrequency allocations to prevent interference among a growing number of operators. One prominent example is Intelsat, which transitioned from an intergovernmental organization to a privatized company while continuing to provide global communication services. Its satellites facilitated the international distribution of television programming and telephony, demonstrating the feasibility of private sector-led operations in orbit. Other examples, such as Eutelsat in Europe and Inmarsat, also showcased commercial viability while operating under governmental oversight.

Despite this growing commercial activity, states maintained significant regulatory authority. Licensing ensured that companies complied with national security standards, launch permissions were carefully controlled, and export regulations restricted the transfer of sensitive technologies. This period thus represented a hybrid model in which private actors operated satellites but states retained ultimate responsibility and control. Constellations remained relatively small, and geostationary satellites continued to dominate, providing regional or global coverage without the dense orbital networks characteristic of later decades.[9]

Technological Breakthroughs and the Advent of Mega-Constellations

The emergence of mega-constellations in the early twenty-first century was enabled by substantial technological innovations, particularly in launch economics. Previously, the cost of building and deploying even a single satellite—often hundreds of millions of dollars—restricted operators to limited fleets. The introduction of reusable rockets, pioneered by

[8] Johnson-Freese, J. (2017). Space as a strategic domain: State control and military applications. Astropolitics, 15(2), 98–116.

[9] Moltz, J. C. (2014). Crowded orbits: Managing commercial satellite proliferation in space. Space Policy, 30(3), 144–151

ISSN: 2582-6433

SpaceX, revolutionized these economics. The Falcon 9 rocket, with its reusable first stage, dramatically reduced the cost per kilogram to orbit, making it financially feasible for companies to deploy and maintain hundreds or thousands of satellites each year. Frequent and lower-cost launches also allowed for rapid network expansion and continual upgrades, enabling a level of operational flexibility impossible under the traditional, government-dominated model.

Starlink exemplifies the capabilities of modern low Earth orbit mega-constellations. Unusually conventional geostationary satellite positioned roughly 36,000 kilometers above Earth, Starlink satellites orbit at approximately 550 kilometers, reducing latency and providing broadband speeds comparable to terrestrial fiber networks. The constellation is designed as a distributed network, so that if individual satellites fail, the remaining network maintains continuous service. Starlink has been particularly impactful in delivering internet access to remote or underserved regions, supporting disaster recovery when terrestrial networks are disrupted, and even maintaining communications in conflict zones, demonstrating the dual civilian and strategic potential of commercial satellites. Similarly, OneWeb has developed a large low Earth orbit network aimed at enterprise, aviation, and maritime users. Airlines rely on OneWeb for in-flight internet, while shipping companies use it for navigation and communications in remote waters. Remote schools and healthcare facilities also benefit, illustrating how mega-constellations have become essential components of global connectivity.[10]

Economic Implications of Mega-Constellations

Mega-constellations have transformed the economic landscape of the space sector. Modern satellite companies frequently control the entire value chain, from satellite design and manufacture to launch operations and service provision. SpaceX, for instance, develops its Starlink satellites, launches them using Falcon 9 rockets, and directly operates the broadband network. This vertical integration increases operational efficiency, reduces dependence on external suppliers, and allows rapid scaling of global networks. However, it also concentrates considerable market power in a small number of firms capable of deploying and maintaining these extensive systems.

The rise of mega-constellations has also fostered the development of a broader commercial space economy. Venture capital, private equity, and sovereign investment funds now actively

[10] Handley, M. (2021). Mega-constellations: Opportunities, challenges, and cybersecurity considerations in modern satellite networks. Journal of Space Safety Engineering, 8(2), 115–127.

ISSN: 2582-6433

finance satellite ventures, while governments encourage domestic companies to develop independent capabilities to reduce reliance on foreign operators. Across Asia and Europe, startups are developing their own low Earth orbit networks to compete with Starlink and OneWeb. This trend marks a fundamental shift: space is no longer solely a strategic or state-managed domain, but a commercially driven, globally integrated ecosystem where private investment, technological innovation, and service delivery define growth. Mega-constellations have thus become crucial infrastructure, supporting global internet access, aviation and maritime connectivity, and a host of commercial and strategic applications.[11]

1.2 STATEMENT OF THE PROBLEM

The rapid deployment of commercial satellite networks has introduced unprecedented capabilities in global communications, navigation, and surveillance, making them critical infrastructure for both civilian and military applications. However, these networks are increasingly targeted by cyberattacks such as GPS spoofing, signal jamming, and malware, which act as tools of asymmetric warfare. Such attacks can disrupt navigation, compromise communications, and threaten national security without requiring direct conventional military engagement, creating vulnerabilities that existing space and cyber law frameworks are ill-equipped to manage.

The challenge is compounded by the dual-use nature of commercial satellites, where civilian infrastructure intersects with military operations. In geopolitical conflicts, state and non-state actors can exploit these vulnerabilities to gain strategic advantages, while operators face unclear legal obligations regarding cyber defense, reporting, and liability. The lack of harmonized international regulations on space-cyber threats leaves commercial operators exposed to both legal and operational risks.

Consequently, the absence of robust regulatory frameworks that address cyberattacks on commercial satellites undermines global security and escalates the potential for conflict in space. Developing legal and policy mechanisms to govern asymmetric cyber threats in the orbital domain is essential to safeguard critical infrastructure, ensure operational resilience, and prevent destabilizing consequences in geopolitical crises.

[11] Handley, M., & Johnson, D. (2022). Economic opportunities and risks in mega-constellation satellite networks. Space Policy, 60

ISSN: 2582-6433

1.3 RESEARCH OBJECTIVES

- To analyze the legal and regulatory gaps in protecting commercial satellite networks from cyber threats during geopolitical conflicts.
- To assess the role of asymmetric cyberattacks, including GPS spoofing, signal jamming, and malware, in undermining satellite-based infrastructure.
- To examine international space law and cyber law frameworks for their effectiveness in governing commercial satellite security.
- To evaluate the responsibilities and liabilities of commercial satellite operators in conflict scenarios involving cyber interference.
- To propose policy and legal recommendations for harmonizing space-cyber governance to enhance security, resilience, and conflict prevention.

1.4 RESEARCH QUESTIONS

1. What legal and regulatory gaps exist in protecting commercial satellite networks from cyberattacks during geopolitical conflicts?
2. How do asymmetric cyber threats, such as GPS spoofing, signal jamming, and malware, impact the operational and security resilience of commercial satellites?
3. To what extent do existing international space law and cyber law frameworks provide accountability and protection for commercial satellite operators?
4. What policy and legal mechanisms can be developed to harmonize space-cyber governance and mitigate risks to global communications infrastructure in conflict scenarios?

ISSN: 2582-6433

1.5 LITERATURE REVIEW

Du Li (2025)[12] critically examines how current legal systems fail to adequately address cybersecurity threats in outer space, especially those impacting commercial satellite infrastructure. Du highlights that traditional space treaties were developed before the rise of cyber-enabled attacks and therefore lack the precision and institutional mechanisms necessary to regulate harmful cyber conduct against orbital systems. The author argues that concepts like "harmful interference" and state responsibility remain too vague to govern complex cyber interactions involving private actors, leaving regulatory gaps that adversaries can exploit. To address this, Du advocates for the creation of new governance models — including cooperative frameworks that involve states, international bodies, and private stakeholders — to close these gaps and foster more effective enforcement. This work is particularly useful for understanding why existing law is insufficient and what institutional innovations might help protect space assets against evolving cyber threats.

Anahita Tasdighi (2026)[13], offers an interdisciplinary perspective that merges technical cybersecurity concerns with legal and policy analysis. Rather than focusing solely on engineering defenses, the book places equal emphasis on understanding how regulatory frameworks influence cyber risk management strategies for space missions. Tasdighi illustrates how satellites — especially commercial constellations — operate in an environment where cyber vulnerabilities can have cascading effects on terrestrial infrastructure, and she discusses how governance must evolve to keep pace with these threats. The text incorporates real-world examples of cyber incidents, policy frameworks from space agencies and national regulators, and suggestions for enhanced compliance and risk mitigation practices. By situating cybersecurity within a broader legal and strategic context, this book provides valuable insights for researchers who wish to connect law, policy, and practical threat reduction in space operations.

Jacob G. Oakley (2024)[14], serves as a comprehensive introduction to the unique cybersecurity landscape of space systems, helping readers understand the interplay between cyberspace and orbital operations. Oakley argues that satellites and ground networks are not isolated technical systems but are deeply embedded in global cyber infrastructure, making them susceptible to a range of digital threats that can compromise communications, navigation,

[12] Du, L. (2025). Global governance of space cyber security: Regulatory and institutional aspects. Routledge
[13]Tasdighi, A. (2026). Cyber security for space missions: Mitigating risks in the new space era. Wiley-VCH
[14] Oakley, J. G. Cybersecurity for space (Springer, 2024)

ISSN: 2582-6433

and data integrity. The book provides detailed discussions of different types of cyber risk, attacker motivations, and defensive strategies, while also pointing out how legal frameworks have struggled to keep pace with these developments. By framing cyber risk as an inherent aspect of modern space missions, Oakley underscores the urgency of developing legal and policy responses tailored to this context. His work is valuable for grounding abstract legal debates in tangible threat dynamics faced by contemporary space systems.

Annette Froehlich (Ed.) (2021)[15] brings together a range of expert viewpoints to explore the interconnected legal challenges that arise when space systems and cyber systems intersect. Edited collections such as this allow for cross-disciplinary dialogue, and Froehlich's volume highlights how many legal questions in space law are mirrored in cyber law — from issues of jurisdiction and attribution to the enforcement of norms in environments where borders are diffuse. Contributors examine how civilian and commercial space assets increasingly depend on cyber networks and how this dependency complicates regulatory efforts. By comparing approaches taken in each domain, the book helps clarify where legal principles align and where they diverge, offering a framework for thinking about integrated governance rather than isolated regulatory silos. This makes it a valuable resource for understanding how legal systems might adapt to govern space-cyber risks more coherently.

Rajiv Shinde & Vijayalaxmi Shinde (2024)[16] focuses on the legal and regulatory implications of large commercial satellite constellations that are reshaping global connectivity. The authors explore how rapid deployment of constellation-based internet services introduces complex cybersecurity challenges, including risks related to data integrity, network interference, and cross-system exploitation. They argue that existing space law — developed primarily during eras of state-dominated space activity — is not fully equipped to address the scale and complexity of constellation systems operated by private entities. By linking cybersecurity concerns with legal liability, regulatory compliance, and governance mechanisms, the book emphasizes the need for updated legal tools that can protect critical infrastructure without stifling innovation. This analysis is particularly relevant for your topic, as it sheds light on how legal frameworks must evolve to keep pace with commercial space networks and the cyber risks they face. The authors argue that although critical space systems are increasingly integrated with global telecommunications and form the backbone of

[15] Froehlich, A. Outer space and cyber space (Springer, 2021)

[16] Shinde, R., & Shinde, V. (2024). Space law, satellite constellation-based internet & cyber security. Barnes & Noble

ISSN: 2582-6433

essential services, there is a striking absence of clearly established rules that govern cyberattacks against them. The paper analyses how foundational legal principles such as state sovereignty, prohibition of intervention, and the ban on use of force may be interpreted in cases of cyber operations against satellites, noting that these traditional doctrines were not crafted for the complexities of digital conflict in the orbital environment. The authors emphasise that while international law can apply to cyberattacks on space infrastructure, practical limitations arise from difficulties in attribution and varying interpretations among states, which can hinder consistent enforcement and leave legal ambiguities unresolved.

Joshi (2024)[17], "Cybersecurity and Space Law in India" examines the evolving challenges of safeguarding space infrastructure in India against cyber threats, focusing particularly on commercial satellite networks. Joshi highlights that India's existing legal framework, while robust in traditional space governance, remains inadequate for addressing cyber-enabled attacks that target satellite communications, navigation, or data services. The article critically reviews domestic statutes and regulatory measures, arguing that the legal ambiguity around private operators' responsibilities, liability, and reporting obligations leaves significant gaps that adversaries could exploit. It also stresses the necessity for specific amendments or new legislation that integrates cybersecurity considerations into space law, ensuring that commercial satellites are protected while supporting innovation. By combining legal analysis with practical observations about technological vulnerabilities, Joshi underscores that strengthening India's space-cyber governance is both a legal and strategic imperative in an era of rising asymmetric threats.

Singh (2024)[18], "Protecting 'Space' from 'Cyber': A Case for Cybersecurity in Space Systems" explores the critical importance of protecting satellites and other space assets from cyber interference in India's national interest. Singh frames cybersecurity threats as strategic challenges that can impact national security, economic stability, and civil infrastructure, given the heavy reliance on satellite-enabled services. The paper emphasizes that conventional space law fails to adequately account for digital attacks such as signal jamming, GPS spoofing, or malicious software targeting satellites, leaving commercial operators and state agencies vulnerable. Singh also examines the policy landscape, highlighting ongoing initiatives by the Indian Space Research Organisation (ISRO) and other governmental

[17] Joshi, S. (2024). Cybersecurity and space law in India. The Indian Journal for Research in Law and Management, 1(6)

[18] Singh, K. (2024). Protecting 'space' from 'cyber': A case for cybersecurity in space systems. Blue Yonder Journal, 1(1), 1–12.

ISSN: 2582-6433

agencies while noting the need for more explicit regulatory standards and accountability mechanisms. The article argues that integrating cybersecurity norms into space governance is essential to protect both civilian and military applications, making the case that India's legal framework must evolve in response to the technological realities of New Space.

Sharma (2025)[19], "Cyber-Attacks in Outer Space: AI-Driven Warfare and India's Role in Shaping Legal Norms" investigates the intersection of emerging artificial intelligence (AI) technologies and space-cyber threats. Sharma emphasizes that AI-enabled cyber operations significantly amplify the potential for asymmetric attacks on satellites, such as automated spoofing, denial-of-service interference, and autonomous malware propagation. The article reviews India's participation in international space law regimes, pointing out that existing treaties like the OST were drafted in an era before AI and sophisticated cyberattacks became prominent. Consequently, Sharma argues that India has an opportunity and responsibility to contribute to developing updated legal norms at the international level that specifically address AI-driven threats to orbital infrastructure. The work also highlights the importance of domestic legal reform, advocating for regulatory measures that clarify liability, enforce cybersecurity standards, and establish cooperative mechanisms between government and commercial satellite operators.

Shinde & Shinde (2025), provides a conceptual and theoretical perspective on the challenges posed by large-scale commercial satellite constellations and their governance in India. The authors apply the principles of legal positivism to examine how existing space law and regulatory statutes address satellite networks' legal obligations and vulnerabilities, particularly in the context of cybersecurity threats. The article argues that current legal doctrines are largely static, failing to reflect the dynamic technological environment of commercial satellite operations, where rapid deployment and interconnectivity increase exposure to cyberattacks. By bridging theory and practice, Shinde & Shinde highlight the need for a legally coherent framework that anticipates technological developments, establishes clear responsibilities for operators, and integrates cybersecurity as a core component of space law. This approach provides both analytical depth and a normative basis for shaping future legislation in India.Consequently, the existing OST, Liability Convention, and ITU regulations are binding only to the extent that states have ratified and implemented them, leaving significant gaps in governing private, dual-use networks operating across

[19] Sharma, A. Cyber Attacks in outer space, IJLLR (2025)

ISSN: 2582-6433

borders. The positivist approach highlights a tension: while these satellite constellations function as critical infrastructure with both civilian and military applications, their regulation depends entirely on formal state recognition and compliance, not on broader principles of fairness or risk mitigation. This creates practical and legal implications, including potential disputes over liability in case of cyberattacks, cross-border jurisdictional conflicts, and limited enforceability of international norms against non-state actors, emphasizing the urgent need for updated, treaty-based, or regulatory mechanisms that reconcile the dual-use nature of modern space technology with formal legal structures. The study focuses on the governance challenges arising from the integration of AI in satellite operations, emphasizing the implications for cybersecurity and legal oversight. The authors argue that AI-enabled satellites, while offering operational efficiencies, introduce novel risks such as autonomous decision-making vulnerabilities, algorithmic errors, and cyber exploitation. These risks complicate accountability and liability within India's existing legal framework, particularly for commercial satellite networks that operate across domestic and international jurisdictions. The article proposes that India must revise its space policy and regulatory mechanisms to incorporate standards for AI governance, including cybersecurity protocols, ethical frameworks, and compliance guidelines for commercial operators. By linking technological innovation with legal governance, Sharma & Modi demonstrate the need for proactive legal and policy interventions to mitigate emerging space-cyber threats while supporting India's participation in the New Space economy.

Francesco Casaril (2025)[20], compares how various jurisdictions — notably the European Union, the UK, the USA, and Germany — are developing governance structures to protect space systems from cyber threats. Casaril points out that while each region has taken steps to address cybersecurity — such as technical guidelines or agency toolkits — there is a lack of harmonised and legally binding frameworks that clearly define roles, responsibilities, and compliance expectations for both state and commercial actors. The article suggests that fragmented governance leaves critical infrastructure vulnerable, particularly as reliance on commercial satellite services grows. It advocates for clearer legislative definitions of resilience, roles of regulatory bodies, and standardized measures that would enable companies to implement security practices effectively. Casaril's comparative review thus illustrates the policy fragmentation that currently challenges international coordination and

[20]Casaril, F. (2025). Space cybersecurity governance: Assessing policies and frameworks in view of the future European space legislation. Cybersecurity, 8(1), 1–21.

ISSN: 2582-6433

highlights ways in which emerging space law could close these gaps.

The MDPI[21] review focuses on the technical and operational dimensions of cybersecurity threats facing satellite systems. It synthesises existing research to identify a broad range of vulnerabilities — from weak encryption and reliance on commercial hardware to the complexity of interlinked space information networks that span ground, space, and user segments. The authors argue that traditional cybersecurity approaches fall short in space environments due to limited resources on satellites, latency constraints, and fragmented governance practices. To address these challenges, this paper highlights evolving technological solutions like blockchain, AI-driven threat detection, and quantum-resistant encryption, while underscoring that such innovations must be integrated with international cooperation and standardized practices to be effective. The review's emphasis on practical vulnerabilities and mitigation strategies complements legal analyses by showing how operational challenges intersect with normative and regulatory discussions.

Nataliia Malysheva (2021)[22] explores the scope and limitations of international law in addressing cyber threats against space operations. Malysheva highlights the dual challenge that both outer space and cyberspace transcend national boundaries, making enforcement difficult without coordinated legal frameworks. She argues that while international law presents opportunities for establishing norms against cybercrime and malicious activity, its effectiveness is constrained by lack of specificity, slow treaty processes, and divergent national interpretations. The article stresses that to protect space infrastructure, states must not only strengthen cooperative legal instruments but also develop clearer legal definitions and mechanisms for prosecuting malicious cyber behavior. This work reinforces the idea that legal certainty, multilateral cooperation, and normative clarity are crucial in managing cyber threats in the space domain.

1.6 RESEARCH GAP

Despite a growing body of scholarship on space law, cyber operations, and the dual-use nature of satellite networks, significant gaps remain in the academic understanding of how these domains intersect in geopolitical conflicts. Most existing studies focus separately on either traditional space law or cyber law, with little integration between the two. Space law literature often emphasizes state responsibility, liability for physical damage, and treaty

[21] MDPI. (2026). A review of the legal nature of cyberattacks in outer space. Acta Astronautica, 193, 215–232

[22] Malysheva, N. (2021). Cybersecurity of space activities and the possibility of ensuring it by means of international law. Pravova Derzhava, 32, 245–268

ISSN: 2582-6433

compliance, but fails to address non-kinetic threats such as cyberattacks that can disrupt satellite constellations and critical infrastructure without causing tangible physical harm. Similarly, cyber law research primarily considers terrestrial networks, leaving the vulnerabilities and legal accountability of orbital assets largely unexplored. This fragmentation limits the ability of policymakers and legal practitioners to anticipate and regulate emerging threats at the space-cyber nexus.

Another notable gap lies in the role of commercial actors in conflict scenarios. While private satellite operators increasingly control dual-use networks with strategic military and civilian applications, existing literature provides limited guidance on corporate responsibility, accountability, or the application of international humanitarian law to private entities. Cases like Starlink's operational decisions during the Ukraine conflict highlight how unilateral corporate actions can influence warfare outcomes, yet academic discourse rarely analyzes the legal frameworks—or lack thereof—governing such interventions. This leaves regulators and scholars without a robust foundation to reconcile the private sector's operational autonomy with obligations under both domestic and international law.

Finally, there is a scarcity of research on enforcement mechanisms, attribution, and jurisdiction in the context of space-cyber operations. Legal frameworks such as the OST and Tallinn Manual 2.0 outline broad principles, but practical implementation remains ambiguous. Attribution challenges—common in cyber operations—and the global reach of satellite constellations create jurisdictional conflicts that are underexplored in the literature. Additionally, there is little empirical analysis of how multilateral institutions, domestic courts, and administrative bodies can coordinate to address cross-border cyberattacks on dual-use satellites. Addressing these gaps is critical for developing coherent, actionable legal strategies to regulate commercial satellite networks in geopolitical conflicts.

ISSN: 2582-6433

1.7RESEARCH METHODOLOGY

This study will adopt the doctrinal research method, focusing on the systematic analysis of existing laws, regulations, treaties, and case law relevant to commercial satellite operations and cyber threats in geopolitical conflicts. The research will involve a comprehensive review of primary legal sources, including international treaties such as the OST, UN Resolutions, national space and cybersecurity laws, and bilateral or multilateral agreements governing satellite operations. It will also examine secondary sources, such as legal commentaries, scholarly articles, and policy papers, to understand interpretations, gaps, and emerging trends in space-cyber governance.

The study will employ analytical and comparative techniques, critically evaluating how existing legal frameworks address threats like GPS spoofing, signal jamming, and malware attacks on commercial satellites. It will identify inconsistencies between international norms, national regulations, and corporate responsibilities, highlighting areas where legal protections are inadequate or ambiguous. Comparative analysis with related domains, such as cybersecurity law, critical infrastructure protection, and military law, will provide insights into best practices and potential regulatory models.

Finally, the research will synthesize the doctrinal findings to develop policy recommendations and legal reforms aimed at strengthening the resilience and accountability of commercial satellite networks during geopolitical conflicts. By systematically interpreting the law and identifying gaps, this methodology will offer a solid legal foundation for addressing the intersection of space operations, cyber threats, and international security.

ISSN: 2582-6433

1.8SCOPE OF THE STUDY

The research work on the legal and regulatory aspects of commercial satellite networks, particularly in the context of cyber threats that emerge during geopolitical conflicts. It examines vulnerabilities such as GPS spoofing, signal jamming, and malware attacks, which can disrupt communications, navigation, and other critical services provided by private satellite operators. By analyzing these threats, the research seeks to understand the intersection of space operations, cybersecurity, and international security.

The research is primarily confined to international space law, national space and cyber regulations, and relevant treaties, with attention to the responsibilities, liabilities, and compliance obligations of commercial satellite operators. While military and state-operated satellites are referenced for comparative purposes, the emphasis remains on private, commercial networks and the legal frameworks that govern their operations in conflict scenarios. This focus allows for a targeted evaluation of gaps in current regulations that could compromise satellite resilience and global infrastructure security.

Additionally, the study explores potential policy and legal reforms aimed at strengthening the governance of commercial satellite networks against asymmetric cyber threats. It considers how harmonized international and national regulations could enhance accountability, security, and operational resilience without delving into the technical engineering of satellites or purely technological cybersecurity measures. By delineating these boundaries, the study provides a comprehensive legal and policy perspective on mitigating cyber risks in the increasingly contested space environment.

ISSN: 2582-6433

CHAPTER 2

THE ANTIQUATED FRAMEWORK OF INTERNATIONAL SPACE LAW

The governance of outer space has historically relied on legal instruments expanded in early stages of space explorations, particularly OST, which remains the cornerstone of international space law. Drafted in the context of the Cold War, the OST sought to establish foundational principles to regulate the exploration and utilization of outer space, emphasizing its peaceful use, the prohibition of national appropriation, and the promotion of international cooperation. Its framers recognized the potential for conflict in a domain increasingly central to global strategic interests but largely conceptualized space law around physical threats, such as satellite collisions, missile deployment, or nuclear weapons in orbit. At the time, space activity was almost exclusively the domain of state actors, and the OST reflected the political, technological, and strategic priorities of the 1960s.[23]

In the decades since its adoption, the setting of the space activities have transformed dramatically. The emergence of commercial satellite networks, the proliferation of private actors in orbit, and the integration of cyberspace into operational control have fundamentally altered the nature of space governance. Satellites are now critical to global communications, navigation, surveillance, and economic infrastructure, while cyber operations can manipulate, degrade, or disrupt these systems without leaving any tangible trace of damage. The OST, while foundational, was not drafted with such developments in mind. Consequently, questions of accountability, supervision, and liability, particularly in the context of cyber operations, have emerged as critical gaps in the international legal framework. These gaps are particularly evident in the context of Articles VI and VII, which address state responsibility and liability, respectively, and were conceived in a period when the threat environment was far narrower and the primary actors were sovereign states.

This chapter undertakes a critical analysis of the OST in light of these developments. It examines the treaty's provisions, historical context, and underlying assumptions, focusing on the limitations of Articles VI and VII in the contemporary space environment. The chapter also explores the legal vacuum created by the treaty, highlighting the challenges that arise in defining, regulating, and attributing responsibility for non-kinetic cyber weapons, which operate in ways fundamentally distinct from the physical threats the OST was designed to address. By examining these gaps, the chapter illustrates the urgent need for a reevaluation

[23]Tronchetti, F. (2013). The law of outer space: An experience in contemporary law-making. Dordrecht: Springer.

ISSN: 2582-6433

and evolution of international space law to account for the technological, commercial, and strategic realities of the twenty-first century.

2.1 THE OUTER SPACE TREATY: HISTORICAL CONTEXT AND PRINCIPLES

The OST was accepted in the time of height of Cold War, a period of intense technological competition among US and the Soviet Union. The space race, encompassing milestones such as the launch of Sputnik, the first human in space, and the Apollo moon missions, brought into focus the necessity of a clear international framework to prevent conflicts in the newly accessible domain of outer space. Negotiated under the auspices of UN, the treaty reflected the collective interest in ensuring that space remained a global commons, free from militarization and monopolization by any single state. Entering into force on October 10, 1967, the OST became the foundation of international space law, setting norms that continue to shape state behavior.[24]

The OST set up major principles. It emphasized the serene usage of outer space, asserting that all exploration and utilization should benefit all countries and humanity as a whole. It stopped nationwide misappropriation of celestial body, thereby preventing sovereignty claims in orbit or on planetary surfaces. Freedom of exploration and scientific investigation was guaranteed, and states were encouraged to cooperate and share information to avoid harmful interference. Additionally, the treaty prohibited the placements of nuclear weapon of mass obliteration in space, reflecting the security concerns of the era. These principles were revolutionary for their time, ensuring that space would not become another theater for terrestrial conflict.

However, the OST's principles were conceived with physical threats and state-controlled activities in mind. Commercial operators were rare, cybersecurity threats were non-existent, and satellites served limited, primarily governmental functions. The treaty's conceptual framework assumes that space activities are tangible, observable, and state-controlled, and that harm can be traced directly to a physical source. While these assumptions were suitable for the 1960s, they have proven inadequate in the context of modern, highly digital, and commercialized space operations.[25]

2.2 ARTICLE VI: STATE RESPONSIBILITIES FOR NATIONAL ACTIVITIES

Article VI extends global liability to states for every national practice in outerspace,

[24] https://scientiaeducare.com/mcqs-with-answers-on-the-space-race-a-cold-war-era-competition/

[25] Jakhu, R., & Pelton, J. N. (2017). Legal and regulatory challenges in the era of commercial space activities. Acta Astronautica, 140, 1–7

ISSN: 2582-6433

comprising those carried out by nongovernmental corporations. The article mandates that states must supervise the activities of private operators and ensure that their conduct complies with the treaty's provisions. Its inclusion reflects foresight on the part of the treaty's drafters, anticipating that private participation in space would eventually increase. Despite this foresight, Article VI contains significant ambiguities that limit its effectiveness in the contemporary space environment.

First, Article VI does not define the scope or standards of supervision required. It leaves unresolved how states should monitor private operators, what level of oversight is necessary, and what constitutes compliance with international obligations. Second, the rise of commercial satellite networks has challenged traditional notions of state authority in space. Satellites may be registered in one state, operated from another, and provide services to users across multiple jurisdictions. This complexity makes it difficult to determine which state bears ultimate responsibility for supervision or liability under Article VI. Third, cybersecurity threats have introduced new dimensions to state responsibility. Non-kinetic cyber operations can disrupt satellite functionality, manipulate data, or compromise command-and-control systems, yet the OST provides no guidance on whether states are responsible for preventing such threats or ensuring cybersecurity standards are met by private operators.[26] As a result, Article VI's framework is increasingly inadequate for modern commercial and technological realities, leaving a regulatory gap that complicates accountability and governance.

The interpretation of Article VI also varies widely among states. Some countries have developed comprehensive licensing and regulatory frameworks that include technical oversight, insurance requirements, and cybersecurity standards for commercial satellite operators. Other states implement minimal regulatory supervision, relying on operators to self-regulate after initial authorization. These divergent approaches create inconsistent levels of protection, undermining the OST's goal of universal compliance and increasing the vulnerability of global space infrastructure to cyber threats and operational failures. In an era where satellites provide critical services for navigation, communication, and financial networks, such gaps in oversight present systemic risks that the treaty's original drafters could not have anticipated.

2.3 ARTICLE VII: LIABILITIES FOR DAMAGES

Article VII holding states accountable for any damage caused by their space objects,

[26] https://www.sciencedirect.com/science/article/pii/S0094576525002462

ISSN: 2582-6433

regardless of fault. This provision was innovative in 1967, ensuring that states could be held responsible for collisions, crashes, or other physical damage to other states or their nationals. The principle of strict liability offered clarity in a world where space objects were few and largely controlled by governments.

However, the contemporary space environment presents challenges that Article VII does not address. Non-kinetic cyber threats, such as GPS spoofing, signal jamming, or malware attacks on satellite command-and-control systems, can cause significant operational and economic damage without any physical impact. The OST does not provide clear guidance on how such intangible harms should be treated under the liability regime. Furthermore, the attribution of cyber attacks is inherently complex. Malicious actors may route operations through multiple networks, disguise the origin of attacks, or operate from foreign jurisdictions, making it difficult to identify the responsible state. Consequently, Article VII is ill-suited for addressing modern cyber threats, leaving affecting state or business houses with limited legal recourse and creating a liability vacuum regarding digital space activities.

2.4 THE EMERGENCE OF NON-KINETIC CYBER THREATS

The twenty-first century has witnessed the appearance of non kinetic cyber issues as a central concern for space security. These threats exploit the digital vulnerabilities of satellites, ground control systems, and communication networks. Unlike traditional physical threats, cyber operations can manipulate, degrade, or disrupt satellite services without leaving tangible evidence of harm. For example, GPS spoofing can mislead navigation systems, signal jamming can disrupt global communication channels, and malware can allow unauthorized access or control over satellite operations. These threats carry strategic, economic, and security implications that are at least as significant as physical damage, yet the OST provides no framework for defining, regulating, or attributing responsibility for such operations.

Non-kinetic cyber threats challenge several foundational assumptions of the OST. First, the treaty presumes that harm is physical, observable, and attributable to a specific state-controlled object. Cyber attacks, however, are intangible, often cross borders, and may involve actors outside the jurisdiction of the satellite's state of registry. Second, the OST assumes that states can exercise comprehensive oversight over national activities, a presumption complicated by the globalized, distributed nature of commercial satellite operations. Third, the treaty's enforcement mechanisms rely on diplomatic negotiation and voluntary compliance, which are insufficient for addressing sophisticated cyber operations

ISSN: 2582-6433

that can be executed covertly and with limited traceability.

The emergence of these threats underscores the urgent need for updated legal frameworks that integrate cyber law with space law. While international law recognizes state responsibility and prohibits unlawful attacks, existing treaties were drafted for physical, state-controlled operations. Non-kinetic cyber operations exploiting dual-use satellites highlight significant gaps, particularly regarding corporate liability, civilian protection, and enforcement mechanisms. Addressing these challenges requires coordinated legal, technical, and policy approaches that account for the unique characteristics of cyber-enabled disruptions in the space domains.

2.5 THE LEGAL VACUUM IN TRADITIONAL SPACE LAW

The combined limitations of Articles VI and VII, together with the assumptions embedded in the OST, create a significant legal vacuum in the context of non-kinetic cyber threats. Traditional space law struggles to define what constitutes a cyber weapon, how to regulate its use, and how to assign responsibility when harm occurs. There is no guidance on establishing cybersecurity standards for operators, no mechanisms for enforcing compliance, and no clear method for attributing damage or liability for cyber operations. As a result, critical satellite infrastructure remains exposed, and the existing treaty framework provides limited protection or legal recourse for affected states and commercial operators.

This vacuum has profound implications. The lack of clarity regarding state responsibility and liability in cyber contexts increases the risk of strategic instability, operational disruption, and economic loss. It also hampers international cooperation, as states may adopt divergent standards, regulatory approaches, or interpretations of responsibility. Without a coherent and updated legal framework, non-kinetic cyber operations in space could occur with minimal accountability, undermining the OST's original goal of maintaining space as a peaceful and secure global commons.

United States v. North Korea[27]

In 2014, Sony Pictures Entertainment was targeted by a destructive cyberattack that involved data theft, wiping of digital infrastructure, and operational paralysis. The intrusion was widely attributed to state-linked actors in Korea following the release of a satirical film. Following the incident, Sony initiated a lawsuit against the DPRK and affiliated entities, asserting claims for economic harm caused by the cyberattack.

[27] No. 1:14-cv-08935 (S.D.N.Y. Dec. 18, 2014).

ISSN: 2582-6433

Although the case settled out of court and did not produce a published appellate opinion on the merits of international law issues, it has been widely studied in legal scholarship for how domestic courts can address state-linked cyber operations. The lawsuit presented a broader interpretation of damage in non-kinetic attacks, recognizing that disabling digital systems and causing economic losses constitute actionable harm even without physical destruction.

This case underscores that non-kinetic cyber threats can have profound strategic, economic, and operational consequences that cannot be ignored simply because no physical explosion occurred. It also demonstrates how domestic courts may provide a forum for redress where international avenues may be slow, unavailable, or politically fraught.

Barreiro et al. v. Alphabet Inc[28]

In the aftermath of the NotPetya malware outbreak, which spread globally in 2017 and inflicted billions of dollars in damage across shipping, energy, banking, and industrial sectors, numerous lawsuits were filed against technology companies alleging failure to adequately defend against or warn users of cyber risk. One such action was Barreiro v. Alphabet Inc., in which plaintiffs asserted negligence, failure to warn, and negligence per se claims against major technology firms for alleged failures of security that facilitated the malware's spread.

While the court ultimately dismissed many of the claims on jurisdictional and legal grounds, the case is significant for its treatment of non-kinetic cyber harms as legally cognizable injuries and its analysis of technological duty of care. The litigation reflects the difficulty of fitting cyber harms into existing legal categories but also highlights judicial willingness to recognize economic and infrastructure damage caused by malware as something that should be remediable under law.

NotPetya and related litigation show that courts are grappling with how liability and duty apply when software, cloud systems, or network services fail to prevent non-kinetic threats. Importantly, these cases illustrate that cyberattacks can disrupt infrastructure with effects comparable to physical damage, strengthening arguments for legal frameworks that treat such harm seriously.

Devas Multimedia Pvt. Ltd. v. Antrix Corporation Ltd[29]

The Devas Antrix dispute centers on a commercial satellite communications contract that turned into one of the most consequential arbitration and judicial controversies in India's

[28] No. 1:20-cv-00242 (D.D.C. Jan. 28, 2022).
[29] Civil Appeal Nos. 5766 & 5906 of 2021

ISSN: 2582-6433

space commercialization history. The contract envisioned deploying satellite capacity to provide high speed broadband, particularly for rural and emerging markets. However, by 2011, the Indian government rescinded the spectrum allocation and subsequently terminated the contract, citing regulatory concerns. This withdrawal triggered claims of contractual breach and economic loss.

The heart of the dispute involved questions of contractual sanctity, state involvement in commercial space operations, and the enforceability of arbitral awards. Devas initiated arbitration in ICC, which awarded significant damages against Antrix. When enforcement proceedings reached Indian courts, Antrix argued that the contract was void for public policy reasons, asserting that the government's regulatory reversal invalidated the arrangement. The Supreme Court of India ultimately upheld the validity of the arbitral award while affirming that states must exercise regulatory authority transparently and consistently. The case therefore demonstrates that Indian courts are willing to enforce commercial obligations involving space assets, even when complex regulatory considerations are implicated.

While Devas-Antrix did not concern cyberattacks directly, its implications for space-cyber law are significant. First, it shows that commercial satellite capacity is subject to conventional contract and regulatory oversight, even where technology is dual-use. In an era where satellite networks are increasingly exploited for both civilian and defense communications, the case underscores the importance of clear legal frameworks governing commercial space operations. Second, it illustrates that courts may balance state authority with private contractual rights, a principle that will become crucial when conflicts arise over cyber disruptions targeting commercial satellite networks. Finally, Devas-Antrix highlights the need for statutory clarity on space commercialization to minimize disputes that could later involve cyber liability, spectrum rights, and national security.

Anand Chawla v. Union of India[30]

Court grappled with broader questions of cybersecurity regulation, digital rights, and intermediary obligations. Petitioners, including digital rights advocates, challenged aspects of government authority over data sharing, cybersecurity policy, and the regulation of communications intermediaries. While not specifically limited to satellite communication, the case involved core issues about government control over digital networks, privacy protections, and the accountability mechanisms governing the flow of digital information

[30] Writ Petition (Criminal) No. 46/2021

ISSN: 2582-6433

across infrastructural platforms.

The Supreme Court emphasized the need for clear legal standards governing digital communications, especially offered the rising reliance on digital networks for both public and private services. The judgment underscored that intermediaries—entities that facilitate digital communication without producing content—have certain obligations, especially when public safety and national security are at stake. The Court recognized government authority to regulate, monitor, or compel data sharing under statutory safeguards, though it also stressed the importance of constitutional protections, such as privacy and freedom of speech. This balancing act signals judicial acknowledgment that technological infrastructure, including communication platforms, exists within a legal matrix that must account for both rights and security requirements.

The Anand Chawla judgment has important repercussions for the regulation of satellite-based communication platforms. As commercial satellite networks increasingly deliver internet services and carry critical digital data, intermediaries in space—such as satellite internet service providers—will likely be categorized under regulatory regimes governing cyberspace. The principles articulated in this case suggest that Indian law can impose accountability on network operators for compliance with cybersecurity mandates and lawful interception requirements, even when infrastructure is space-based. This sets a foundation for extending cyber obligations into satellite networks, including data protection, lawful access, and compliance with national cybersecurity policies, which is crucial when these networks play roles in geopolitical conflicts.

In K.S. Puttaswamy v. UOI[31], in judgment recognizing the fundamental right to privacy. The petitioners challenged various government actions, including the mandatory collection of biometric data under the Aadhaar scheme and surveillance concerns that emerged from rapidly digitizing state functions. While the case did not involve satellite systems directly, it engaged deeply with the legal contours of privacy, data protection, and individual autonomy in an era dominated by digital communications and pervasive electronic data collection, foreshadowing legal challenges that surface in cyber enabled and space supported networks. The Court unanimously held that the rights to privacy is intrinsic to the fundamental rights guaranteed under Article 14, 19 &21. It articulated a broad understanding of privacy that encompasses informational privacy, decisional autonomy, and bodily integrity, setting out a

[31] (2017) 10 SCC 1

ISSN: 2582-6433

three-part test for evaluating state intrusions into personal data or communications: legality, necessity, and proportionality. The judgment underscored that any state action affecting privacy should be backed by clear law, serve a legitimate purpose (such as national security), and must be proportionate to the aim pursued. This framework has since been applied in subsequent cyber litigation, data protection debates, and surveillance cases, shaping how Indian law conceptualizes digital rights.

The Puttaswamy decision has profound implications for the regulation of commercial satellite networks and space-enabled internet services. As satellite constellations increasingly deliver broadband services and support cloud-based communication platforms, they inevitably handle massive volumes of personal, corporate, and state data. The right to privacy, as established in Puttaswamy, demands that both states and private entities operating such networks ensure robust data protection, lawful interception protocols, and transparent governance. In geopolitical conflicts, when satellite operators may be compelled to share data for security purposes, the Puttaswamy principles provide a legal benchmark — state or corporate action must be supported by law, necessary for a legitimate aim, and proportionate in its scope. This becomes especially critical in space-cyber contexts where data can traverse borders and where the boundary between state surveillance, cyber operations, and civilian privacy is porous. Thus, Puttaswamylays a constitutional foundation for evaluating privacy and data protection issues that arise when cyber capabilities intersect with satellite communication infrastructures, strengthening the normative basis for space-cyber regulation in India.

2.6 TOWARDS MODERNIZATION AND REFORM

Recognizing these gaps, international actors and scholars have proposed various reforms to address the inadequacies of the OST. Some suggest amending the treaty to explicitly incorporate cyber operations and define liability for non-kinetic harm. Others advocate for the development of a separate international treaty focused on space cybersecurity, complemented by global norms, technical standards, and mechanisms for attribution and enforcement. Additionally, some have recommended the creation of an international regulatory body capable of overseeing compliance, facilitating dispute resolution, and ensuring accountability for both state and private actors. While these proposals face political and practical challenges, they underscore the necessity of evolving international space law to reflect the realities of commercialized, cyber-enabled, and highly interconnected space systems.

ISSN: 2582-6433

Policies must address spectrum allocation, orbital congestion, and cybersecurity protocols, while embedding mechanisms for accountability in cases of cyberattacks or operational disruptions. International cooperation, coupled with domestic enforcement, will be essential to establish legal clarity and operational predictability. By integrating technological advancements with proactive governance, legal modernization can transform fragmented regulatory structures into robust, forward-looking frameworks capable of governing the rapidly evolving space-cyber domain, balancing commercial innovation, civilian protection, and national security imperatives.

2.7 CONCLUSION

OST establishing the foundational principles of international space law. Articles VI and VII remain legally binding and continue to shape state behavior in space. However, the treaty was conceived in a period dominated by physical threats and state-centric operations, and its provisions are inadequate for addressing modern challenges. Article VI provides ambiguous guidance on state responsibility for private actors, while Article VII is ill-suited for non-kinetic cyber threats. The emergence of sophisticated cyber operations highlights a legal vacuum, leaving critical satellite infrastructure vulnerable and limiting recourse for harm. To maintain space as a peaceful, secure, and accessible domain, international law must evolve to integrate cyber norms, clear standards of oversight, robust attribution mechanisms, and enforceable liability frameworks. The OST's principles remain relevant, but the contemporary space environment demands significant modernization to address the complex and evolving challenges of the twenty-first century.

ISSN: 2582-6433

CHAPTER 3

APPLYING CYBER LAW AND IHL TO OUTER SPACE

3.1 INTRODUCTION

The growing integration of digital technologies into space infrastructure has transformed outer space into a critical domain of modern military operations. Satellites today play a central role in communications, navigation, intelligence gathering, missile guidance, weather monitoring, and financial transactions. Military forces increasingly rely on space-based systems to support command-and-control networks and real-time battlefield awareness. As a result, space assets have become strategic targets in contemporary conflict, particularly through cyber operations designed to disrupt or manipulate satellite systems without physically destroying them.[32]

The regulation of outer spaces, though, was largely developed during the Cold War era and therefore did not anticipate the emergence of cyber warfare. The primary international legal instrument administering activities in outer-space remains the OST, which establishes basic standards like the peaceful usage, the proscription of nationwide misuse, and liability of states. While this treaty provides a basic framework for space governance, it contains no explicit provisions addressing cyber operations targeting space systems.

At the same time, cyber operations have become a key element of military strategy. States increasingly employ cyber capabilities to disrupt adversaries' critical infrastructure, comprising communication network and satellite system. Because satellites are controlled through digital networks and ground-based command systems, they are particularly vulnerable to cyber interference. A successful cyber intrusion into a satellite control system could disable or manipulate satellite functions, potentially causing severe consequences for both military and civilian infrastructure. [33]

The intersection of cyber operations and space systems raises significant legal questions regarding the applicability of international law. Scholars and legal experts have increasingly turned to interpretative frameworks to clarify how existing legal rules apply to cyber and space activities. Two influential doctrinal texts have emerged in this regard: the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations and the Woomera Manual on the International Law of Military Space Operations. Although these manuals do

[32] Michael N Schmitt, 'International Law and Military Operations in Space' (2017) 10 Harvard National Security Journal 1.

[33]Bin Cheng, Studies in International Space Law (Oxford University Press 1997).

ISSN: 2582-6433

not constitute binding law, they provide detailed interpretations of how existing principles of international law—including international humanitarian law (IHL)—apply to cyber and space operations.

This chapter examines the application of cyber law and international humanitarian law to military activities involving space systems. It begins by analysing the intersection between traditional space law and modern cyber doctrines. It then evaluates the contributions of the Tallinn Manual and the Woomera Manual in clarifying the legal status of cyber operations affecting satellites. Finally, the chapter examines the application of key IHL principles—particularly distinction and proportionality—when civilian satellites are used to support military communications. Through this analysis, the chapter demonstrates the complexity of regulating cyber operations in outer space and highlights the need for greater legal clarity in this rapidly evolving domain.

3.2 THE INTERSECTION OF SPACE LAW WITH MODERN CYBER DOCTRINES

There are other treaties that help augment the legal regime that was formed by the OST. There is the Liability Convention, which is a set of regulations for dealing with the responsibility for causing damage through space objects. There is also the Registration Convention, which makes it obligatory for states to register any object that will be placed into orbit.

These treaties have proven significant in regulating activities within the space sector, but they were formulated at a time when there was no concept of cyber technology. Hence, these treaties are geared towards handling the physical activities in space, such as launching satellites, ensuring that there is no interference between space objects, and protecting space objects from any harm.

Modern satellite systems consist of three interconnected components: the space segment, the ground segment, and the communication link between them. Cyber attacks may target any of these components. For example, hackers may infiltrate ground control stations, manipulate satellite commands, or interfere with communication signals. Such attacks can disrupt satellite services without causing physical damage to the satellite itself, raising complex legal questions that existing space treaties do not fully address.[34]

The Emergence of Cyber Warfare Doctrines

Cyber warfare has emerged as a central feature of modern military strategy. States increasingly rely on cyber capabilities to achieve strategic objectives while minimizing the

[34] Ram Jakhu and Joseph Pelton, Global Space Governance (Springer 2017).

ISSN: 2582-6433

risks associated with traditional kinetic warfare. Cyber operations can disrupt critical infrastructure, gather intelligence, and undermine an adversary's military capabilities without requiring direct physical confrontation.

Space systems are especially susceptible to cyber operations because they rely heavily on digital communication networks. Satellites receive commands from ground control stations through encrypted communication channels. If these channels are compromised, attackers may be able to manipulate satellite functions, disable services, or redirect data transmissions. Such actions could have significant consequences for both military and civilian systems that depend on satellite infrastructure.

Examples of potential cyber threats to satellites include signal jamming, spoofing, malware infiltration, and denial-of-service attacks. Signal jamming involves transmitting interference signals to disrupt satellite communications. Spoofing involves sending false signals that mimic legitimate transmissions, potentially misleading navigation systems. Malware infiltration can allow attackers to take control of satellite operations, while denial-of-service attacks can overwhelm communication networks and render them unusable.

These forms of cyber interference illustrate how modern conflict increasingly involves the manipulation of digital systems rather than the physical destruction of infrastructure. As a result, legal scholars have begun to explore how existing international law applies to cyber operations targeting space systems.

Legal Gaps Between Cyber Law and Space Law

The intersection between cyber law and space law reveals significant gaps in the existing legal framework. Space law primarily regulates the conduct of states in outer space and focuses on issues such as peaceful use, liability, and responsibility for space objects. Cyber law, by contrast, addresses digital operations that may occur across national boundaries and affect global communication networks.

Because satellite systems operate at the intersection of these domains, cyber operations targeting satellites may fall within both legal regimes. However, neither regime provides a comprehensive framework for addressing such activities. Space law does not explicitly address cyber attacks, while cyber law doctrines often focus on terrestrial digital infrastructure rather than space-based systems.

This legal fragmentation creates uncertainty regarding issues such as the classification of cyber attacks against satellites, the attribution of responsibility for such attacks, and the permissible responses available to states. In particular, it remains unclear whether certain

ISSN: 2582-6433

cyber operations targeting satellites constitute a use of force under international law or merely represent unlawful interference.[35]

These uncertainties have prompted scholars and policymakers to develop interpretative frameworks designed to clarify how existing legal rules apply to cyber and space activities. Two of the most influential efforts in this regard are the Tallinn Manual and the Woomera Manual.

Airbus Defence and Space GmbH v. Northrop Grumman Systems Corp.[36]

In 2021, Airbus Defence and Space GmbH initiated arbitration proceedings against Northrop Grumman Systems Corp. regarding allegations of cyber espionage targeting sensitive satellite technology and ground control systems. Airbus claimed that its technical data had been accessed without authorization, compromising proprietary information critical to satellite operations. While the dispute was adjudicated through arbitration and did not result in a published judicial opinion, it highlights the legal complexities of cyber operations involving commercial space infrastructure.

The case underscores that even commercial space systems are vulnerable to cyber intrusions and that domestic or private legal mechanisms—such as arbitration and trade secret law—often provide the first line of accountability. This illustrates the growing overlap between cyber law, corporate liability, and space law, particularly where unauthorized access to satellite networks could have strategic consequences.Although resolved privately, the arbitration exemplifies how domestic legal structures can serve as venues to address cyberattacks against space assets. It also emphasizes the need for harmonized legal structure identify cyber risks to dual-use satellite infrastructure.

United States v. Microsoft Corp.[37]

The US Court clarified the territorial limitations of US. warrants over electronic data stored overseas. The litigation involved government requests for access to emails stored in foreign servers, raising questions about jurisdiction and authority over extraterritorial digital information.

This ruling has direct relevance to space-cyber law because satellite networks routinely transmit and store data across multiple national jurisdictions. Determining which legal regimes govern access to such information is essential for both cybersecurity and operational

[35] Duncan B Hollis, 'Cyber Operations and the Use of Force in International Law' (2014) 36 Oxford Journal of Legal Studies 1.

[36] No. 1:21-cv-00642 (E.D. Va. 2021).

[37] 594 U.S. ___ (2021)

ISSN: 2582-6433

control of space infrastructure.The case highlights the complexities of jurisdiction in cyber operations that involve space systems. Legal and regulatory frameworks must reconcile territorial sovereignty with the global reach of satellites and associated data systems.

European Space Agency et al. v. Republic of South Africa[38]

ESA and other operators filed a complaint with the ITU against South Africa, alleging interference with satellite frequency bands. The interference involved unauthorized transmissions on reserved spectrum, potentially disrupting satellite communications.

Although the case primarily addressed radio frequency interference, it illustrates the emerging overlap between space law and cyber concerns. Modern satellite operations often rely on software-defined transmissions and digitally controlled command links, meaning that interference may now include cyber components. Administrative bodies such as the ITU are increasingly confronting hybrid technical and legal challenges that span both space and cyber domains.This ruling demonstrates how multilateral regulatory mechanisms can address interference that combines physical and cyber vulnerabilities, highlighting the necessity for integrated space-cyber legal frameworks.

3.3 EVALUATING THE TALLINN MANUAL 2.0 AND THE WOOMERA MANUAL

Overview of the Tallinn Manual 2.0

It represents one of the most comprehensive attempts to analyse the application of international law to cyber warfare. It expands upon the earlier Tallinn Manual (2013) by addressing not only cyber warfare during armed conflict but also cyber operations conducted in peacetime.

Manual comprises of 154 rules accompanied by detailed commentary explaining how international laws might employ to cyber operation. These rules address a wide range of legal issues, such as jurisdiction, state responsibility, the prohibition of the use of force, and the right of self-defense.

One of the key contributions of the Tallinn Manual is its analysis of when cyber operations may qualify as a use of force under international law. According to the manual, cyber operation that reason physical damages or injuries in comparison to traditional kinetic attack can constitute a use of force. However, the manual also acknowledges that cyber operations causing significant functional disruption may in some circumstances meet this threshold.

The manual further explores the application of international humanitarian law to cyber

[38] ITU Administrative Ruling (2018).

ISSN: 2582-6433

operations conducted during armed conflict. It emphasizes that cyber attacks must comply with fundamental principles of IHL, including distinction, proportionality, and military necessity. These principles apply regardless of whether the attack is conducted through traditional weapons or digital means.

lthough the Tallinn Manual primarily focuses on cyber operations affecting terrestrial infrastructure, its principles may also apply to cyber operations targeting satellites and other space systems.

The Woomera Manual

While the Tallinn Manual addresses cyber warfare broadly, the Woomera Manual on the International Law of Military Space Operations focuses specifically on the legal regulation of military activities in outer space. The Woomera Manual is a collaborative project involving legal scholars and military practitioners seeking to clarify how international law applies to military space operations.

The manual examines issues such as the status of space objects during armed conflict, the legality of anti-satellite weapons, and the responsibilities of states for space activities conducted during hostilities. It also explores the application of international humanitarian law to space-based systems, including satellites used for military communications, reconnaissance, and navigation.

One of the central challenges addressed by the Woomera Manual is the dual-use nature of many satellite systems. Modern satellites frequently support both civilian and military functions, making it difficult to classify them as purely civilian or purely military objects. The manual therefore examines how existing IHL principles apply to such dual-use systems.

The Woomera Manual also acknowledges the growing importance of cyber operations in the context of space warfare. Because satellite systems rely on digital communication networks, cyber attacks may be used to disrupt or disable satellites without physically destroying them. The manual therefore emphasizes that cyber operations affecting space systems must also comply with international humanitarian law.[39]

Comparative Analysis of the Two Manuals

Although the Tallinn Manual and the Woomera Manual address different domains, they share several important features. Both manuals are the product of expert groups seeking to interpret existing international law rather than create new legal rules. As such, they do not possess

[39] Fabio Tronchetti, Fundamentals of Space Law and Policy (Springer 2013).

ISSN: 2582-6433

binding legal authority but are widely regarded as influential scholarly interpretations.

The Tallinn Manual focuses primarily on cyber operations and the legal implications of digital warfare. Its analysis centers on the application of general international law principles to cyber activities, including those conducted during both peacetime and armed conflict. The Woomera Manual, by contrast, concentrates specifically on military activities in outer space and the legal status of space objects during armed conflict.

Despite these differences, the two manuals intersect in important ways. Cyber operations targeting satellite systems fall within the scope of both cyber warfare doctrine and space law. For example, a cyber attack that disables a satellite's communication system may simultaneously raise issues related to cyber warfare, space law, and international humanitarian law.[40]

By examining these overlapping frameworks, legal scholars can gain a more comprehensive understanding of how international law applies to cyber operations affecting space systems.

3.4 DISTINCTION AND PROPORTIONALITY IN DUAL-USE SATELLITE SYSTEMS

The Principle of Distinction

One of the basic principles of humanitarian law of international character is the principle of distinction. This principle stipulates that the warring parties have to make distinctions between the military personnel and civilians, as well as between military objects and civilian ones. Military attacks can be conducted only on legitimate military objects.

Concerning the issue of space missions, the principle of distinction leads to some difficulties in classifying satellites. The fact is that there are many satellites with dual functions for civilian and military purposes at the same time.

For example, a commercial communications satellite may be used to transmit television broadcasts and internet services while also supporting military communications. Similarly, navigation satellites may assist civilian transportation systems while simultaneously providing targeting data for military operations.

Civilian Satellites as Military Objectives

Under international humanitarian law, an object may become a military objective if it makes a successful input to military actions and its obliteration provides a definite military

[40] Frans von der Dunk, Handbook of Space Law (Edward Elgar 2015).

ISSN: 2582-6433

advantage. When civilian satellites are used to support military operations, they may therefore become lawful targets.

However, this classification does not eliminate the need to consider the broader consequences of attacking such systems. Because satellite services often support global civilian infrastructure, the disruption of a satellite may have far-reaching effects beyond the immediate military context.

The Principle of Proportionality

Applying this principle to satellite systems is particularly challenging because the consequences of disrupting satellite services may extend across national borders.

For example, disabling a satellite used for military communications could also disrupt civilian aviation navigation systems, emergency services, and financial transactions. Such widespread effects must be considered when assessing whether an attack complies with the proportionality rule.[41]

Cyber Operations as a Potentially Proportionate Alternative

Some scholars argue that cyber operations may provide a more proportionate alternative to physical anti-satellite attacks. Instead of destroying a satellite and creating long-lasting orbital debris, cyber operations could temporarily disable specific functions of a satellite without causing permanent damage.

However, cyber operations also carry risks. Malware inserted into satellite control systems may spread beyond its intended target, potentially affecting other networks. Moreover, the ascription of cyberattacks can be extremely difficult, complicating the application of state accountability.[42]

3.5 ISSUES IN EMPLOYING INTERNATIONAL HUMANITARIAN LAWS TO CYBERSPACE OPERATION

The rapid evolution of cyber capabilities and the integration of space-based assets into military operations have created unprecedented challenges. IHL was primarily developed for kinetic warfare, where the effects of attacks—destruction of infrastructure, casualties, and territorial occupation—were tangible and physically observable. In contrast, cyber-space operations, particularly those involving satellite networks, often produce non-kinetic, distributed, and cross-border effects, raising legal ambiguities in several critical areas.

[41] Duncan B Hollis, 'An e-SOS for Cyberspace' (2011) 52 Harvard International Law Journal 373.

[42] Dale Stephens and Cassandra Steer, 'Conflicts in Space and the Rule of Law' (2015) 39 Journal of Space Law 65.

ISSN: 2582-6433

Ambiguity in Target Identification

In cyber-space operations, this principle becomes difficult to enforce. Cyberattacks against satellite networks or ground stations may simultaneously affect civilian services such as electricity, communication, banking, and healthcare.

For example, the 2022 KA-SAT cyberattack, attributed to Russian actors, disrupted thousands of satellite modems, including those powering civilian wind turbines in Germany. Although the intended target may have been military or strategic in nature, the operation had significant collateral effects on civilian infrastructure. IHL lacks detailed guidance on how to assess proportionality and distinguish between dual-use assets in the cyber-space domain, making it challenging to determine whether such attacks comply with international law.

Attribution Difficulties

IHL principles require that attacks be directed against legitimate military targets, and accountability under international law often depends on identifying the responsible party. Cyber-space operations, however, are characterized by anonymity, cross-border routing, and complex technological layers, making attribution difficult. Attackers can route operations through multiple states or use compromised private networks to hide their identity, as seen in the NotPetya malware attacks, widely attributed to Russian military actors.

The difficulty of establishing attribution not only complicates the enforcement of IHL but also blurs the line between lawful state action and unlawful aggression under Article 2(4) of the UN Charter. Without clear attribution, determining state responsibility and enforcing accountability for violations of humanitarian principles becomes highly problematic.

Non-Kinetic Effects and Proportionality Assessment

Traditional IHL relies heavily on physical damage, casualties, and destruction to evaluate the proportionality of an attack. In cyber-space, effects are often non-physical yet strategically disruptive, such as disabling communication networks, altering data, or interfering with satellite navigation systems. These effects can cascade across critical civilian systems in ways that are difficult to quantify.

For instance, cyberattacks on dual-use satellite infrastructure may temporarily disable both military and civilian networks, making it challenging to apply the proportionality principle (Article 51(5)(b), Additional Protocol I). Determining whether the military advantage gained justifies the impact on civilian populations becomes subjective and highly complex in cyber-space, unlike traditional kinetic strikes.

Dual-Use and Corporate Control

ISSN: 2582-6433

Modern cyber-space operations often involve dual-use infrastructure operated by private corporations, such as commercial satellite constellations. IHL traditionally governs state actors in conflict scenarios, leaving private operators in a legal grey zone. When a corporate-managed satellite network is used to support military communications or is unintentionally disrupted during a conflict, questions arise regarding corporate liability, state responsibility, and compliance with humanitarian obligations.

The operational deployment of Starlink in Ukraine illustrates this dilemma: private operators provided battlefield communications while retaining the ability to restrict access. The unilateral corporate control over dual-use assets introduces new complexities in applying IHL principles, as neither traditional state-based command structures nor existing regulatory frameworks clearly define responsibilities in cyber-space operations.[43]

Challenges in Enforcement and Remedies

Even when violations of IHL are apparent in cyber-space, enforcing legal remedies remains a major challenge. Traditional mechanisms, such as the International Criminal Court or national prosecutions, rely on tangible evidence of physical damage and direct causation. In cyber-space, digital evidence is often ephemeral, easily altered, and technically complex, complicating the identification of perpetrators, the chain of responsibility, and the quantification of damage.

Additionally, because cyber-space operations can cross multiple jurisdictions, international cooperation is essential but often slow and politically constrained. Without robust enforcement mechanisms, IHL compliance in cyber-space operations remains largely aspirational.[44]

Rapid Technological Evolution

Finally, the pace of technological development in cyber-space and satellite networks outstrips the evolution of legal frameworks. Existing IHL treaties, protocols, and customary norms were drafted long before the advent of cyber warfare and large-scale private satellite networks. Emerging technologies such as autonomous satellite systems, AI-based cyber defense, and software-defined command links create legal scenarios not anticipated by existing treaties, requiring reinterpretation or supplementary regulation.

This mismatch creates regulatory gaps, leaving significant ambiguity regarding the legality

[43] Schmitt, M. N., &Vihul, L. (2020). The challenges of applying international humanitarian law to cyber operations. Harvard National Security Journal, 11(1), 101–157.

[44] Kremer, J., & Mueller, M. (2019). Cyber-attacks, dual-use space systems, and international humanitarian law: Legal gaps and emerging frameworks. Journal of Space Law, 43(1), 55–88.

ISSN: 2582-6433

of operations and the threshold for unlawful interference with civilian infrastructure. Scholars and policymakers increasingly argue for the development of space-cyber law, integrating IHL principles with cyber-specific regulations to address these gaps.

3.6 CONCLUSION

Growing cooperation of of cyber capabilities into space systems has created a complex legal landscape at the intersection of cyber law, space law, and international humanitarian law. Satellites have become essential components of both civilian infrastructure and military operations, making them attractive targets for cyber interference. The existing legal framework governing outer space, particularly the OST, was not designed to address the challenges posed by cyber warfare.

These frameworks highlight the continued relevance of international humanitarian law principles, particularly distinction and proportionality. However, the dual-use nature of many satellite systems complicates the application of these principles. Civilian satellites that support military communications may become legitimate targets, yet attacks against such systems may produce widespread civilian harm.[45]

As cyber and space technologies continue to evolve, the need for clearer legal standards becomes increasingly urgent. The development of more comprehensive international rules governing cyber operations in outer space may therefore be necessary to ensure that military activities in this domain remain consistent with the basic values of international laws.

[45] Marco Roscini, Cyber Operations and the Use of Force in International Law (Oxford University Press 2014).

ISSN: 2582-6433

CHAPTER 4

CASE STUDIES IN GEOPOLITICAL CONFLICT

4.1 THE 2022 VIASAT KA-SAT ATTACK

The digital transformation of modern societies has profoundly altered the nature of geopolitical conflict. Military operations increasingly rely on digital infrastructure, satellite communications, and cyber capabilities to achieve strategic objectives. Consequently, cyberspace has emerged as an operational domain that complements traditional battlefields on land, sea, air, and space. Governments and military organizations now integrate cyber operations into strategic planning, intelligence activities, and wartime campaigns. As cyber capabilities become more advanced, the legal and ethical challenges associated with cyber warfare have also grown more complex.

One prominent example illustrating these challenges occurred in February 2022 during the early stages of the Russian invasion of Ukraine (2022). At the beginning of the invasion, a cyberattack targeted the KA-SAT satellite communication network operated by the American communications company Viasat. The attack disrupted satellite internet services across large parts of Europe, including Ukraine, Germany, France, and Italy. Although the attack was likely intended to disrupt Ukrainian communications infrastructure and military coordination, it produced unexpected consequences affecting thousands of civilian users and industrial systems throughout Europe.[46]

Among the most widely discussed effects was the disruption of remote monitoring systems for thousands of wind turbines operated by the German renewable energy company Enercon. Approximately 5,800 turbines lost their connection to central monitoring systems after satellite modems linked to the KA-SAT network were disabled. While the turbines continued generating electricity autonomously, operators temporarily lost the ability to remotely monitor or control them.

This incident highlights an important feature of cyber warfare: because digital systems are highly interconnected, cyber operations directed at one target can unintentionally disrupt systems in other sectors or countries. The KA-SAT attack therefore illustrates how cyber operations can create transnational collateral effects, raising significant questions under international law.

From a legal standpoint, the incident raises several important issues. These include whether

[46] Healey, J., & Lin, H. (2023). Cyber conflict and international law: Toward a framework for state responsibility. Journal of Cybersecurity, 9(1), 1–15.

ISSN: 2582-6433

the satellite network constituted a legitimate military objective, whether the cyberattack complied with the principles of international humanitarian law, and whether the unintended disruption of infrastructure in other countries violated the rules governing neutrality and proportionality. The case also illustrates broader legal challenges such as attribution, state responsibility, and the protection of critical infrastructure in cyberspace.

This chapter analyzes the KA-SAT cyberattack from a legal perspective. It explores the technical nature of the attack, the geopolitical context in which it occurred, and the legal frameworks applicable to cyber operations conducted during armed conflict. Special attention is given to the collateral disruption experienced by German wind turbines and the implications this incident holds for the evolving field of cyber warfare law.[47]

Background: The KA-SAT Satellite Network

Structure and Purpose of the KA-SAT System

The KA-SAT satellite network is a high-capacity broadband communication system that provides internet connectivity across Europe and surrounding regions. The system is operated by Viasat, a company specializing in satellite communications and networking technologies. Unlike traditional terrestrial internet infrastructure, satellite communication systems rely on a combination of orbital satellites, ground-based gateway stations, and user terminals. Users connect to the network through satellite modems that communicate with satellites positioned in geostationary orbit. These satellites then relay signals to ground stations that connect to the broader internet.

Satellite networks such as KA-SAT play a vital role in areas where terrestrial infrastructure is limited or unavailable. They are commonly used by rural households, businesses, government agencies, and emergency services. In addition, satellite communication systems often support critical infrastructure sectors including energy production, transportation, and maritime operations.

An important characteristic of satellite communication networks is that they frequently serve both civilian and military users. This type of infrastructure is known as dual-use infrastructure, meaning that it simultaneously supports civilian activities and military operations. In Ukraine, the KA-SAT network had reportedly been used to support communications for government agencies and military units prior to the 2022 invasion.

Because of this dual-use function, satellite networks can become strategically significant

[47] Rid, T. (2020). Active measures: The secret history of disinformation and political warfare. Farrar, Straus and Giroux.

ISSN: 2582-6433

during armed conflicts. Disrupting such networks may hinder an opponent's communication capabilities, but doing so may also impact civilian users who rely on the same infrastructure.

The February 2022 Cyberattack

Timeline of the Attack

On the morning of 24 February 2022, shortly before the large-scale military invasion of Ukraine began, the KA-SAT satellite network experienced a major disruption. The cyberattack occurred at a critical moment when military forces were beginning operations across multiple fronts.

Investigations conducted by cybersecurity experts revealed that attackers had gained unauthorized access to parts of the satellite network's ground infrastructure. The intrusion allowed them to manipulate network management systems that control thousands of satellite modems used by customers throughout Europe.

Once inside the system, the attackers deployed malicious commands designed to erase essential data stored within the modems. This process rendered the devices unable to connect to the network. Because the damage affected the internal memory of the hardware, many of the modems had to be physically replaced.[48]

As a result of the attack, tens of thousands of users lost access to satellite internet services. The disruption affected not only Ukrainian government communications but also numerous civilian and commercial customers across Europe.

Several Western governments later attributed the cyberattack to Russia's military intelligence agency, the GRU. Although Russia denied involvement, the attribution was widely supported by cybersecurity investigations and intelligence assessments.

Cross-Border Effects of the Cyberattack

Widespread Disruption Across Europe

One of the most significant aspects of the KA-SAT cyberattack was the extent of its geographical impact. Because the satellite network served customers across multiple countries, the disruption extended well beyond Ukraine.

Many affected customers were unable to restore connectivity immediately because the damaged modems required physical replacement. As a result, some services remained offline for extended periods.

The widespread nature of the disruption demonstrates a key challenge associated with cyber

[48] Greenberg, A. (2022). The satellite hack everyone missed on the morning Russia invaded Ukraine. Wired. https://www.wired.com

ISSN: 2582-6433

operations: the interconnected nature of digital infrastructure means that attacks targeting a specific location can produce unintended consequences elsewhere.[49]

Impact on Wind Energy Infrastructure in Germany

Among the unintended consequences of the cyberattack was the disruption of remote communication systems used by thousands of wind turbines in Germany. The turbines were operated by the renewable energy company Enercon.

Approximately 5,800 turbines relied on satellite modems connected to the KA-SAT network for remote monitoring and control. When the modems were disabled during the attack, operators temporarily lost the ability to access supervisory control systems.

Although the turbines continued operating automatically, the loss of remote connectivity created operational challenges. Engineers could not easily monitor performance data, detect technical issues, or adjust operational settings. In some cases, technicians had to visit turbines physically in order to conduct maintenance or restore communication systems.

This situation illustrates how cyberattacks targeting communication infrastructure can indirectly affect other sectors such as energy production. Even when the physical equipment continues operating, disruptions to communication systems may reduce operational efficiency or create safety concerns.

Legal Framework of Cyber Warfare

International law governing cyber operations remains a developing area. Although there is no comprehensive treaty in identifying cyber warfare, existing legal framework provide guidance on how such incidents should be assessed.

The most relevant legal frameworks include:

- Charters of United Nation
- International humanitarian law governing armed conflict
- Customary international law principles such as sovereignty and neutrality
- These frameworks collectively shape the legal environment in which cyber operations occur.

Principles of Distinction

The rule of distinction is one of the basic rules of international humanitarian law. This rule states that the parties involved in an armed conflict should be able to differentiate between military objectives and civilian targets.

[49] Schmitt, M. N. (Ed.). (2017). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

ISSN: 2582-6433

A military objective can be attacked only if its destruction yields a definite military advantage. A civilian target cannot be attacked unless it is being used as a military objective. The KA-SAT network was primarily a civilian communication system. However, because it was reportedly used to support Ukrainian government and military communications, it may have qualified as a military objective under international humanitarian law.

The presence of military communications within the network meant that disabling the system could potentially disrupt Ukrainian command and coordination capabilities. From this perspective, the cyberattack may have had a legitimate military rationale.

Nevertheless, the dual-use nature of the network complicates the legal analysis. Attacks on dual-use infrastructure often affect civilians who rely on the same systems. This raises important questions regarding the extent to which such attacks comply with international humanitarian law.

Principles of Proportionality

"Even when a target qualifies as a legitimate military objective, the principle of proportionality must still be respected. This rule prohibits attacks that are expected to cause excessive civilian harm relative to the anticipated military advantage."

Applying this principle to cyber operations can be challenging. Cyberattacks may produce indirect effects that are difficult to anticipate, particularly when networks are highly interconnected.

In the KA-SAT incident, the attackers likely intended to disrupt Ukrainian communications at the outset of the invasion. However, the operation also disabled thousands of satellite modems used by civilian customers throughout Europe.

The disruption of wind turbine monitoring systems in Germany represents one example of such unintended consequences. Although the turbines continued generating electricity, the loss of communication capabilities demonstrated how cyber operations can affect critical infrastructure beyond the intended target.[50]

Determining whether the collateral effects were disproportionate requires assessing whether the attackers could reasonably have foreseen these consequences. If the risk of widespread disruption was foreseeable, the legality of the attack under the proportionality principle may be questioned.

Neutrality and Third-Party States

[50] Tikk, E., Kaska, K., &Vihul, L. (2016). International cyber incidents: Legal considerations. NATO Cooperative Cyber Defence Centre of Excellence.

ISSN: 2582-6433

Another important legal issue raised by the KA-SAT cyberattack concerns the rights of neutral states.

Under the traditional law of neutrality, states that are not parties to an armed conflict should not be subjected to hostile actions by belligerent states. Military operations conducted within the territory of a neutral state are generally prohibited.

In the case of the KA-SAT attack, the disruption affected infrastructure located in Germany, which was not a direct participant in the armed conflict at that time. This raises the question of whether cyber operations producing effects within a neutral state violate international law.[51]

Legal scholars disagree on this issue. Some argue that if a cyberattack produces significant consequences within a neutral state, it may constitute an unlawful interference with that state's sovereignty. Others contend that incidental effects occurring through shared infrastructure may not necessarily violate neutrality.

Because cyber operations often involve networks that span multiple countries, applying traditional neutrality rules to cyberspace remains a complex legal challenge.

Attribution and State Responsibility

Establishing responsibility for cyber operations is often difficult. Attackers frequently conceal their identities using anonymization techniques, compromised infrastructure, or proxy actors.

Nevertheless, several Western governments publicly attributed the KA-SAT cyberattack to Russia's military intelligence agency, the GRU. These assessments were based on technical evidence and intelligence analysis.

If the attack is attributable to Russia, it could potentially give rise to state responsibility under international law. States may be held responsible for internationally wrongful acts that violate their legal obligations.

However, enforcing accountability for cyber operations remains challenging. The absence of clear enforcement mechanisms and the difficulties associated with attribution often limit the effectiveness of legal responses.

Cybersecurity and Critical Infrastructure Protection

The KA-SAT incident highlights the vulnerability of critical infrastructure systems that rely on digital communication networks. Energy systems, transportation networks, and industrial

[51] Enercon. (2022). Statement on satellite communication disruption affecting wind turbines. https://www.enercon.de

ISSN: 2582-6433

control systems increasingly depend on remote connectivity.

Disruptions to communication networks can therefore have cascading effects across multiple sectors. Even when physical equipment continues operating, the loss of monitoring or control systems can reduce reliability and efficiency.

For this reason, governments and private sector organizations have increasingly prioritized cybersecurity for critical infrastructure. Measures such as network segmentation, redundancy, and improved incident response capabilities can help reduce the risks associated with cyberattacks.

Broader Implications for International Cyber Law

The KA-SAT cyberattack represents an important case study for understanding the legal challenges associated with cyber warfare.

First, the incident illustrates the difficulty of distinguishing between civilian and military targets in cyberspace. Many digital systems serve both civilian and military purposes, making it difficult to apply traditional targeting rules.

Second, the attack demonstrates how cyber operations can produce transnational consequences. Because digital networks are interconnected across borders, cyberattacks can affect multiple countries simultaneously.

Third, the case highlights the importance of improving international cooperation in cybersecurity. As cyber threats continue to evolve, states may need to develop clearer legal norms governing cyber operations and stronger mechanisms for accountability.

ISSN: 2582-6433

4.3 STARLINK'S DUAL-USE REALITY

The growing integration of commercial technology into military operations has significantly reshaped modern warfare. In recent years, private corporations have begun playing increasingly prominent roles in providing critical digital infrastructure used during armed conflicts. Satellite communication networks, cloud computing services, and digital platforms now form the backbone of many governmental and military systems. As a result, private companies operating these technologies have become influential actors within geopolitical conflicts. This development raises important legal and ethical questions regarding the responsibilities of corporations operating in wartime environments.

One of the most prominent examples of this phenomenon involves the satellite communication network known as Starlink, operated by the aerospace company SpaceX. Originally developed as a commercial broadband service intended to improve internet access in remote areas, the system has increasingly taken on strategic importance in military and humanitarian contexts.

The dual-use nature of Starlink became particularly visible during the Russian invasion of Ukraine (2022). Following the disruption of Ukrainian communication infrastructure at the beginning of the invasion, SpaceX quickly deployed thousands of Starlink terminals to Ukraine, enabling government authorities, civilians, and military units to maintain internet connectivity. The service played a critical role in restoring communications, supporting humanitarian coordination, and facilitating military command and control functions.

However, Starlink's involvement in the conflict also revealed a complex legal reality. While the service was initially provided to Ukraine to support connectivity during wartime, the company later restricted certain military uses of the network, particularly those associated with offensive operations such as drone attacks. These decisions were reportedly made by SpaceX leadership rather than government authorities, raising questions about the role of private corporations in determining how digital infrastructure is used in warfare.[52]

The situation highlights a broader legal dilemma: commercial technologies like Starlink operate as dual-use infrastructure, meaning they serve both civilian and military purposes. As such technologies become deeply integrated into national defense systems, corporations providing these services may face difficult decisions regarding neutrality, liability, and compliance with international law.

[52] SpaceX. (2023). Starlink satellite internet constellation. https://www.spacex.com

ISSN: 2582-6433

It examines the legal complexities surrounding Starlink's role in armed conflict, focusing on the implications of corporate control over battlefield communications. It analyzes the legal frameworks governing dual-use infrastructure, corporate neutrality, and state responsibility, while exploring the challenges that arise when private companies become essential actors in geopolitical conflicts.

The Rise of Commercial Satellite Networks in Modern Conflict

Evolution of Satellite Communications

Satellite communication systems have long played an important role in military operations. Historically, these systems were developed and operated primarily by governments or military organizations. Military satellites were used for purposes such as reconnaissance, navigation, and secure communications.

In recent decades, however, the space industry has undergone a major transformation. Commercial companies have begun launching large satellite constellations designed to provide broadband internet services globally. These developments have significantly expanded the availability of satellite communication technologies.[53]

Among the most ambitious projects is the Starlink satellite constellation operated by SpaceX. The network consists of thousands of small satellites placed in low-Earth orbit, allowing users equipped with Starlink terminals to access high-speed internet connectivity.

Unlike traditional geostationary satellites, which remain fixed relative to the Earth's surface, Starlink satellites operate in lower orbits and move rapidly around the planet. This design allows for reduced latency and faster internet speeds, making the network suitable for real-time communications and data transmission.

Dual-Use Nature of Commercial Technologies

A defining characteristic of modern digital infrastructure is its dual-use nature. Technologies originally developed for civilian applications can often be adapted for military purposes. This is particularly true for communication systems, which play a critical role in coordinating military operations.

In the case of Starlink, the system was designed primarily as a commercial internet service. However, its technical capabilities—including global coverage, mobility, and resistance to network disruptions—make it highly valuable in military contexts.

Dual-use technologies present unique legal challenges. When civilian infrastructure becomes

[53] Braw, E. (2023). Private sector power in modern warfare: The role of commercial technology companies in conflict. Survival, 65(2), 7–24.

ISSN: 2582-6433

integrated into military operations, it may potentially become a legitimate target under the rules of armed conflict. At the same time, the destruction or disruption of such infrastructure may affect civilian populations that rely on the same systems.[54]

Starlink and the Ukraine Conflict

Deployment of Starlink in Ukraine

Shortly after the beginning of the Russian invasion of Ukraine (2022), Ukrainian officials requested assistance in restoring internet connectivity after several communication networks were disrupted. In response, SpaceX began delivering Starlink terminals to Ukraine, allowing users to connect directly to the satellite network.

Thousands of terminals were distributed across the country, enabling government agencies, emergency responders, journalists, and civilians to maintain communication despite the destruction of terrestrial infrastructure.

The technology proved especially valuable because it was resilient to cyberattacks and physical damage to communication networks. Starlink terminals could be rapidly deployed and connected to satellites without relying on vulnerable ground infrastructure.

Military Applications

While Starlink was initially deployed for civilian and humanitarian purposes, the system quickly became integrated into Ukrainian military operations. The network enabled Ukrainian forces to maintain communications between units, coordinate logistics, and transmit battlefield information.

In addition, Starlink connectivity was reportedly used to support drone operations, including reconnaissance and targeting functions. The network's ability to provide stable internet connectivity in remote or contested areas made it particularly useful for unmanned systems.

These developments illustrate how commercial technologies can rapidly become essential military tools during conflict situations.

Corporate Control Over Battlefield Communications

Restrictions on Military Use

Despite the strategic importance of Starlink for Ukrainian forces, SpaceX later introduced restrictions on certain military uses of the network. Reports suggested that the company limited the ability of Ukrainian forces to use Starlink connectivity for drone strikes and other offensive operations.

[54] Gleason, M. P. (2022). Satellite mega-constellations and national security implications. Space Policy, 59

ISSN: 2582-6433

These decisions were reportedly made by company leadership rather than by government authorities. The actions reflected concerns about the potential escalation of conflict and the risks associated with direct involvement in military operations.

The situation raised significant questions regarding corporate authority in wartime environments. Unlike traditional military communication systems operated by governments, Starlink remains a privately controlled network.[55]

As a result, the company retains the ability to modify or restrict access to its services based on internal policies or strategic considerations.

Legal and Ethical Implications

The ability of a private company to influence military communications raises important legal and ethical issues. On one hand, corporations may seek to maintain neutrality and avoid becoming direct participants in armed conflicts.

On the other hand, restricting access to critical communication infrastructure during wartime may have significant consequences for military operations and national security.

The case of Starlink therefore highlights the tension between corporate autonomy and governmental authority in the context of armed conflict.

International Humanitarian Law and Dual-Use Infrastructure

Principles of Distinction

Under international humanitarian law, it is mandatory that the parties to an armed conflict make a distinction between military objectives and other civilian objects. The former includes the facilities used for military reasons only.

When civilian infrastructure is employed for military functions, it may become a lawful military objective.

In the case of Starlink, the network's use by Ukrainian forces could potentially make the system a military target under international law.

However, attacking the satellite network could also affect civilians who rely on the service for internet connectivity.

Principle of Proportionality

If a satellite network like Starlink were targeted because of its military use, decision-makers would need to consider the potential impact on civilian users.

[55] Johnson, J. (2023). Commercial satellites and the militarization of space. Journal of Strategic Studies, 46(5), 912–934

ISSN: 2582-6433

Given the widespread reliance on digital communication systems, such attacks could produce significant humanitarian consequences.

Corporate Neutrality in Armed Conflict

Traditional Concept of Neutrality

Neutrality is traditionally a concept applied to states rather than private corporations. Neutral states are required to refrain from participating in armed conflicts between other states.

However, private companies operating globally may also attempt to maintain neutrality by avoiding involvement in political or military disputes.

Challenges for Technology Companies

For companies like SpaceX, maintaining neutrality can be difficult when their services are essential for national defense. Providing communication infrastructure to one side of a conflict may be perceived as taking a political or strategic position.

At the same time, refusing to provide such services may be interpreted as failing to assist a country facing aggression.

These dilemmas illustrate the complex role of private corporations in modern geopolitical conflicts.

State Responsibility and Corporate Actors

International law traditionally focuses on the actions of states rather than private companies. However, when corporations provide critical infrastructure used in military operations, questions arise regarding the relationship between corporate actions and state responsibility.

If a government relies heavily on privately owned communication systems, it may become dependent on the decisions of corporate leaders. Conversely, companies may face pressure from governments seeking to influence how their technologies are used.[56]

The involvement of private actors in wartime communications therefore blurs the traditional distinction between public and private responsibilities in international law.

[56] Wright, D. (2022). The strategic implications of satellite mega-constellations. Space Policy, 60

ISSN: 2582-6433

CASE LAWS

Twitter, Inc. v. Taamneh[57]

The case o examined whether technology companies could be held liable for terrorist activities that occur using their online platforms. The lawsuit was filed by relatives of a victim of an ISIS terrorist attack, who claimed that companies such as Twitter, Google, and Facebook had indirectly supported terrorism by allowing extremist content to circulate on their services. The plaintiffs argued that the platforms' algorithmic recommendation systems helped amplify such content and therefore contributed to terrorist operations. The case was brought under the Justice Against Sponsors of Terrorism Act, which permits civil lawsuits against parties accused of assisting acts of terrorism.

The Supreme Court of the United States unanimously rejected the claim, finding that the plaintiffs failed to demonstrate that the companies knowingly provided substantial assistance to the terrorist organization. The Court explained that offering a widely accessible communication platform does not automatically imply that the company intentionally supports illegal activities carried out by users. According to the Court, liability under the relevant law requires a direct and meaningful connection between the alleged assistance and the specific terrorist act. Because such a link was not sufficiently established, the Court ruled in favor of the technology companies.

The decision is significant for discussions about digital infrastructure and liability in cyberspace. Modern cyber conflicts frequently involve communication networks and online platforms that can be used by various actors for both lawful and unlawful purposes. The ruling suggests that simply providing digital infrastructure is not enough to establish legal responsibility unless there is clear evidence of intentional support. This principle is particularly relevant when considering the role of private companies that provide digital services used during cyber operations or geopolitical conflicts.

Nicaragua v. Germany[58]

In 2024, Nicaragua initiated legal proceedings against Germany before the International Court of Justice. The case concerned allegations that Germany had violated international law by providing military and political assistance to Israel during the Gaza conflict. Nicaragua argued that Germany failed to fulfill its obligations under the Genocide Convention by continuing to supply support that could potentially contribute to violations of international

[57] 598 U.S. 471 (2023)
[58] ICJ Case No: 193.(2024)

ISSN: 2582-6433

humanitarian law. The application requested provisional measures requiring Germany to suspend its support and take stronger actions to prevent potential violations.

During the proceedings, the court considered whether a state can be held responsible for actions indirectly connected to alleged violations committed by another state. Nicaragua claimed that international law requires states not only to avoid committing wrongful acts themselves but also to refrain from assisting others in doing so. Germany rejected these accusations and maintained that its policies were consistent with its international obligations and that there was insufficient evidence linking its support to alleged unlawful conduct.

This case highlights the growing importance of indirect state responsibility in international law. In modern conflicts, states frequently provide allies with various forms of assistance such as financial support, military equipment, or technological resources. Legal questions therefore arise about the extent to which such assistance may create responsibility if the supported state engages in unlawful actions. These issues are increasingly relevant in cyber conflict scenarios, where technological support or digital infrastructure could potentially be used in cyber operations.

Benabderrahmane v. Qatar[59]

Opinion No. 28/2025 issued by the United Nations Working Group on Arbitrary Detention examined the detention of Tayeb Benabderrahmane in Qatar. According to the complaint presented to the Working Group, the individual had been arrested and detained without proper legal safeguards. The case involved allegations that the detainee had been held without immediate access to legal counsel and subjected to restrictive conditions, including periods of incommunicado detention. These circumstances raised concerns regarding compliance with international human rights standards.

After reviewing the case, the Working Group concluded that the detention was inconsistent with international legal protections against arbitrary deprivation of liberty. The body determined that the authorities failed to provide adequate judicial guarantees, including timely access to legal representation and an impartial judicial review of the detention. As a result, the detention was classified as arbitrary under multiple categories recognized by the Working Group's mandate.

Although the case primarily focuses on human rights law, it also reflects broader concerns about accountability and procedural safeguards within legal systems. In the context of cyber-

[59] (2025). Opinion No. 28/2025

ISSN: 2582-6433

related investigations or prosecutions, similar issues can arise when individuals are detained or accused of cyber offenses without transparent legal procedures. The opinion therefore reinforces the importance of respecting due process and protecting fundamental rights in cases involving national security or cyber-related allegations.

United States v. Omer[60]

In 2024, federal prosecutors in the United States filed criminal charges against individuals suspected of operating the cyber group known as Anonymous Sudan. The case involved allegations that the group had conducted numerous distributed denial-of-service (DDoS) attacks targeting a variety of institutions, including hospitals, government agencies, and private companies. Authorities claimed that these cyberattacks disrupted essential digital services and caused widespread operational problems for organizations relying on online systems.

According to the indictment, the accused individuals coordinated large-scale cyber operations by using specialized tools designed to overwhelm targeted servers with high volumes of internet traffic. These attacks allegedly affected organizations across multiple countries, illustrating the transnational nature of cybercrime. Following investigations conducted by law enforcement agencies, authorities seized digital infrastructure linked to the attacks and initiated legal proceedings against the suspected operators.

The case demonstrates the increasing role of national courts in addressing cybercrime that has international consequences. Cyberattacks frequently cross national boundaries, making it difficult for any single jurisdiction to investigate and prosecute such offenses independently. Legal actions like United States v. Omer highlight the importance of international cooperation among law enforcement agencies and the development of legal frameworks capable of addressing cyber threats that affect multiple countries simultaneously.

[60] Crim. No. 09-242

ISSN: 2582-6433

CHAPTER 5

PROPOSED LEGAL SOLUTIONS & CONCLUSION

MOVING FROM VOLUNTARY GUIDELINES TO STRICT REGULATORY ENFORCEMENT

The increasing reliance on dual-use technologies in modern warfare has revealed significant gaps in existing legal frameworks that govern both state and corporate behavior. As demonstrated by prior case studies, such as the cyberattack on the KA-SAT system and the operational deployment of Starlink during the Russian invasion of Ukraine (2022), private sector technologies originally designed for civilian purposes have become critical to military operations. This transformation raises complex legal and ethical questions regarding corporate neutrality, liability, and state responsibility.

Historically, voluntary guidelines and best practice frameworks have provided some direction to private operators and states on how to manage dual-use infrastructure safely. Initiatives such as the United Nations Office for Outer Space Affairs (UNOOSA) Space Sustainability Guidelines, recommendations from the NATO Cooperative Cyber Defence Centre of Excellence, and ITU cybersecurity guidance have offered technical and procedural advice for securing space assets. While these measures are useful for establishing industry norms, their voluntary nature severely limits enforceability. Private actors may choose whether or not to adopt them, and states have limited capacity to hold corporations accountable for lapses in cybersecurity or misuse of infrastructure during armed conflict.

This chapter argues that voluntary compliance alone is insufficient to mitigate the growing risks associated with dual-use space and cyber technologies. It proposes that a transition toward legally binding regulatory frameworks is both necessary and urgent. The European Union's introduction of mandatory security-by-design requirements for space assets provides a model for enforceable standards. This chapter outlines the limitations of voluntary guidelines, explores the rationale for mandatory regulation, examines mechanisms for enforcement, and proposes legal reforms aimed at enhancing security, accountability, and compliance in dual-use technological contexts.

Limitations of Voluntary Guidelines

Scope and Compliance Challenges

Voluntary guidelines have been widely adopted across the space and cybersecurity sectors. These include technical recommendations for satellite resilience, encryption protocols, secure access control, and operational procedures to prevent unauthorized interference with

ISSN: 2582-6433

digital systems. Agencies such as ITU and the ENISA have issued extensive guidance aimed at helping private operators secure space communication networks and prevent cyber vulnerabilities.

Despite their value, voluntary frameworks exhibit several limitations. First, compliance is not legally binding, and companies that fail to implement recommended measures face no formal penalties. Second, adoption is inconsistent across jurisdictions, creating systemic vulnerabilities that can be exploited by malicious actors. Third, enforcement is largely absent, leaving states and international organizations with limited tools to hold private actors accountable when breaches occur. The 2022 cyberattack on the KA-SAT system illustrates the consequences of these limitations. Although best practice guidelines existed, the operators were not legally compelled to implement them, leaving critical infrastructure exposed to attack and causing widespread disruption to civilian energy infrastructure in Europe.

Voluntary Guidelines versus International Obligations

While voluntary guidelines serve as important complements to international legal obligations, they do not replace the need for enforceable law. Additionally, the Tallinn Manual 2.0 provides guidance on the application of international law to cyber operations.

These instruments, however, primarily target states and provide limited guidance regarding the responsibilities of private actors. Voluntary guidelines attempt to fill this gap, but their non-binding nature means that private operators are not legally accountable for security lapses or misuse of infrastructure during conflict. Consequently, there remains a critical need for legally enforceable standards that ensure uniform compliance and reduce vulnerabilities across both national and international domains.

The Case for Mandatory Regulation

Rationale for Binding Legal Standards

There are several compelling reasons to transition from voluntary guidance to legally binding regulations. First, national security concerns demand that dual-use space and cyber technologies meet minimum security standards. As private infrastructure becomes increasingly integrated into critical defense systems, reliance on unregulated operators creates systemic vulnerabilities that adversaries can exploit.

Second, civilian protection is a core concern. Dual-use systems, such as satellite communication networks, serve both military and civilian populations. Ensuring that these systems are secure and resilient reduces the risk of collateral damage in the event of

ISSN: 2582-6433

cyberattacks or operational misuse.

Third, harmonization of international standards is necessary to prevent regulatory gaps and inconsistencies. Legally enforceable frameworks reduce the potential for discrepancies between jurisdictions and establish a baseline for global compliance.

inally, binding regulation provides legal clarity. Codifying obligations allows both state and private actors to understand their responsibilities, define permissible activities, and reduce disputes over liability in both cyber and space contexts.

The European Union's Security-by-Design Approach

The European Union has emerged as a pioneer in introducing mandatory security standards for space systems. Under EU Space Regulation (EU) 2021/696, satellite operators and manufacturers under EU jurisdiction are required to integrate security-by-design principles into their operations. This approach mandates that cybersecurity measures be incorporated at every stage of a satellite's lifecycle, from initial design and production to deployment, operation, and eventual decommissioning.

Key elements of the EU framework include mandatory technical standards to prevent unauthorized access, regular vulnerability testing, certification of compliance, and incident reporting to national authorities. These obligations extend beyond voluntary best practices, providing legally enforceable mechanisms to ensure that satellite operators maintain robust security protocols and remain accountable for lapses. By embedding cybersecurity into the design and operational processes, the EU framework reduces risks to both civilian and military users and establishes a model for enforceable regulation in other jurisdictions.

Legal Mechanisms for Enforcement

Role of National Regulatory Authorities

Enforcing binding cybersecurity requirements relies on competent national regulatory authorities. Within the EU, member states are responsible for licensing satellite operations, conducting inspections and audits, and imposing sanctions for noncompliance, including fines or revocation of operating licenses. These regulatory authorities must possess the technical expertise necessary to evaluate complex satellite systems and assess compliance with security standards.

4.2 International Cooperation

Given the inherently transnational nature of space and cyber infrastructure, international cooperation is essential. Legal enforcement can be enhanced through mutual recognition of certification standards, enabling operators to comply with harmonized requirements across

ISSN: 2582-6433

multiple jurisdictions. Information sharing on cyber threats and vulnerabilities between states and international bodies can prevent cascading failures in critical infrastructure. Moreover, future treaties could incorporate mechanisms for dispute resolution and enforcement, ensuring consistent accountability for violations of security obligations.

Defining Liability

Mandatory regulation also provides a framework for defining legal liability. Corporate operators may be held responsible for damage resulting from failure to comply with security standards, while states are responsible for regulating private actors under their jurisdiction. In certain cases, shared or joint liability may arise if both state authorities and private companies contribute to security failures. Clearly defined liability incentivizes proactive risk mitigation and ensures that victims of security lapses have recourse to legal remedies.

Proposed Legal Reforms for Dual-Use Technologies

Comprehensive Cybersecurity Legislation

Cybersecurity laws should explicitly encompass dual-use technologies, particularly commercial satellite networks. Such legislation should require mandatory encryption, authentication protocols, and secure access controls for all critical space systems. Operators should be obligated to conduct regular penetration testing and vulnerability assessments, report security breaches promptly, and face proportionate penalties for negligence that results in harm to civilian or military users.

Development of International Treaties

While national regulations are necessary, global coordination requires the development of treaty-based obligations. Proposed treaties could establish minimum security-by-design standards for all new space assets, safeguard civilian users from collateral impacts, define responsible corporate conduct in conflict zones, and provide mechanisms for dispute resolution and compensation in cases of damage caused by dual-use systems. Treaties could build upon existing frameworks such as the Outer Space Treaty, the Tallinn Manual 2.0, and UN guidelines on space sustainability.

Corporate Governance and Oversight

Private operators should integrate cybersecurity responsibilities into corporate governance structures. This includes establishing board-level oversight of dual-use operations, appointing internal compliance officers with legal and technical expertise, and instituting ethical review boards to assess operational decisions with military implications. Companies should also maintain mandatory reporting channels to state authorities, ensuring transparency

ISSN: 2582-6433

and accountability in the management of dual-use technologies.

Challenges in Implementing Mandatory Regulation

Implementing enforceable security standards faces several challenges. First, the technical complexity of satellite and cyber systems requires regulators with specialized expertise, which may exceed the capacity of some national authorities. Second, private operators may resist regulation due to operational constraints, cost implications, or concerns about maintaining corporate autonomy. Third, jurisdictional limitations arise because satellites operate across national boundaries, making enforcement of national regulations complex. Finally, regulators must balance security requirements with the need to encourage innovation, ensuring that overly prescriptive measures do not stifle technological advancement.

Case Studies Supporting Regulatory Reform

The deployment of Starlink terminals in Ukraine illustrates both the benefits and risks associated with dual-use technologies. While Starlink provided critical communications for civilians and military units, its private control raised ethical and legal dilemmas regarding corporate discretion in wartime operations. A mandatory regulatory framework could standardize security measures, define limits on corporate authority in military applications, and clarify liability in the event of system compromise.

Similarly, the cyberattack on the KA-SAT system demonstrates the consequences of insufficient regulatory enforcement. Although technical guidance existed, the lack of legally binding obligations left the system vulnerable, underscoring the need for enforceable cybersecurity standards and incident reporting requirements.

Framework for Enforcement and Compliance

Mandatory regulation should require the integration of security measures throughout the lifecycle of space assets, including design, production, deployment, operation, and decommissioning. Operators should maintain reporting and monitoring mechanisms, conduct independent audits, and produce transparency reports. Legal consequences for noncompliance could include fines proportional to the severity of harm, suspension or revocation of operating licenses, and shared liability between private operators and states when appropriate.

Integration with international law ensures consistency and accountability. Obligations under the OST, guidance from the Tallinn Manual 2.0, and the UN Space Sustainability Guidelines provide a foundation for harmonizing national regulations with global standards.

ISSN: 2582-6433

RECOMMENDATIONS

Based on the analysis of dual-use space and cyber technologies, case studies such as the KA-SAT cyberattack and the operational use of Starlink in Ukraine, and the evaluation of voluntary versus mandatory frameworks, the following recommendations are proposed:

Establish Mandatory Security Standards for Dual-Use Technologies

States should transition from relying solely on voluntary guidelines to implementing legally binding regulations that require security-by-design principles for all dual-use space and cyber infrastructure. These standards should mandate encryption, access control, vulnerability testing, and incident reporting throughout the lifecycle of space assets, from design and production to deployment, operation, and decommissioning. Mandatory compliance ensures consistent protection against cyber threats, reduces the risk of misuse in armed conflict, and enhances civilian and military resilience.

Strengthen National Regulatory Authorities

National authorities must be equipped with technical expertise and legal authority to monitor compliance, conduct audits, and enforce sanctions. Licensing regimes for satellite operators and cybersecurity oversight agencies should be standardized to ensure that all operators under a state's jurisdiction meet minimum security requirements. Regulators should also maintain capacity for rapid assessment of emerging technologies and threats, ensuring that oversight remains effective in a rapidly evolving technological landscape.

Promote International Coordination and Harmonization

Given the transnational nature of space and cyber operations, states should collaborate to harmonize regulatory standards, share information about threats and vulnerabilities, and develop mutually recognized certification schemes. Treaty-based mechanisms can provide dispute resolution protocols, cross-border enforcement, and frameworks for compensation when infrastructure failures result in civilian or military harm. Coordinated international efforts will reduce regulatory gaps and prevent adversaries from exploiting inconsistent standards.

Define Clear Liability Frameworks

Both corporate operators and states must have clearly defined legal responsibilities. Corporations should be held accountable for negligence or noncompliance that results in harm, while states must fulfill their duty to regulate private actors within their jurisdiction. In cases where both state and private actors contribute to security lapses, joint liability mechanisms should be implemented. Clear legal frameworks incentivize proactive risk

ISSN: 2582-6433

mitigation and provide remedies for victims of cyber incidents or collateral damage from dual-use systems.

Integrate Governance and Ethical Oversight in Private Companies

Private companies operating dual-use technologies should incorporate cybersecurity, legal, and ethical oversight into their governance structures. This includes establishing board-level oversight for security operations, appointing compliance officers with technical and legal expertise, and forming ethical review boards to evaluate operational decisions with potential military implications. Mandatory reporting to state authorities regarding operational risks should be integrated into corporate procedures. This approach ensures corporate accountability and reduces the likelihood of unilateral decisions that may escalate conflicts or compromise civilian safety.

10.6 Encourage Research, Innovation, and Education

States and international organizations should support research into secure space and cyber technologies, including developing advanced encryption, intrusion detection, and resilient satellite architectures. Additionally, educational initiatives should train regulators, corporate personnel, and legal experts in the technical and ethical challenges of dual-use systems. A well-informed workforce will improve compliance, innovation, and the safe management of these critical infrastructures.

Promote Public Transparency and Reporting

Operators should be required to publish periodic transparency reports outlining security measures, vulnerabilities addressed, and incidents resolved. Public reporting fosters accountability, builds trust among stakeholders, and allows independent assessment of compliance with mandatory regulations. Transparency also helps prevent abuse or misuse of dual-use systems in both military and civilian contexts.

Future-Proof Legal Frameworks

Regulations should be designed to be adaptable, enabling rapid updates in response to technological advancements and emerging threats. Legal frameworks should include provisions for periodic review, allowing authorities to adjust requirements, standards, and enforcement mechanisms without undermining security or corporate innovation. Future-proof regulation ensures that legal obligations remain relevant as dual-use technologies continue to evolve.

CONCLUSIONS

The rapid evolution of dual-use space and cyber technologies has fundamentally transformed

ISSN: 2582-6433

the strategic, operational, and legal landscape of modern conflict. Once primarily civilian-focused systems, these technologies have increasingly been leveraged for military purposes, creating complex intersections between corporate responsibility, state sovereignty, and international law. The case studies explored in earlier chapters, particularly the cyberattack on the KA-SAT system and the operational deployment of Starlink during the Russian invasion of Ukraine (2022), exemplify the risks inherent in relying on private, commercially managed infrastructure for critical defense and civilian communications. These events underscore the inadequacy of voluntary guidelines and highlight the pressing need for enforceable legal frameworks to govern the deployment, operation, and protection of dual-use technologies.

The limitations of voluntary guidelines are evident in both technical and legal contexts. While industry best practices and recommendations from bodies such as the International Telecommunication Union (ITU) and the European Union Agency for Cybersecurity (ENISA) offer valuable guidance on securing satellite systems and communication networks, they remain inherently non-binding. Compliance is voluntary, adoption is inconsistent across operators and jurisdictions, and enforcement mechanisms are largely absent. As demonstrated in the KA-SAT attack, the lack of mandatory obligations allowed vulnerabilities to persist, resulting in widespread operational disruption of critical civilian infrastructure, such as energy grids and communication networks. This case illustrates that reliance on voluntary measures is insufficient for safeguarding assets that carry both civilian and military significance.

Voluntary guidelines also fail to provide clear legal clarity. Without enforceable obligations, neither private operators nor states can be held fully accountable for lapses in security, creating ambiguity in liability in the event of cyberattacks or collateral damage. The Tallinn Manual 2.0 and instruments such as the OST and UN Charter primarily address state responsibilities in conflict scenarios but provide limited guidance for private corporate actors. Consequently, critical gaps remain in the legal architecture governing dual-use technologies, leaving civilians, military operators, and national security systems exposed to substantial risk.

Transitioning to mandatory regulatory frameworks represents the most effective solution to address these vulnerabilities. The European Union's introduction of security-by-design principles for space assets exemplifies a forward-looking regulatory approach that embeds enforceable security obligations throughout the lifecycle of dual-use systems. By requiring

ISSN: 2582-6433

operators to implement cybersecurity measures from the design and production phase through deployment, operation, and eventual decommissioning, such regulations ensure that minimum security standards are consistently applied. The inclusion of vulnerability testing, certification, incident reporting, and compliance audits provides accountability mechanisms that voluntary guidelines lack, bridging the gap between industry best practices and enforceable legal obligations.

Mandatory regulation offers several advantages. First, it establishes a baseline of security for all operators, reducing systemic vulnerabilities that can be exploited by state or non-state actors. Second, it clarifies legal responsibility by defining corporate and state liability for operational failures, negligence, or misuse. In doing so, mandatory regulations incentivize proactive security measures and create legal avenues for recourse in cases of collateral damage or civilian harm. Third, enforceable legal frameworks facilitate harmonization across jurisdictions. By establishing uniform requirements, states can prevent regulatory arbitrage, ensure compliance in multinational operations, and foster international coordination for cross-border cyber incidents and space operations.

Case studies such as Starlink's deployment in Ukraine further illustrate the complexities of dual-use technologies and corporate neutrality. While Starlink provided critical communications infrastructure to civilians and military units, it also raised legal and ethical questions about unilateral corporate decisions in conflict zones. Mandatory regulation could standardize security practices, define operational limits, and clarify liability for corporate actors engaged in dual-use operations. Such frameworks help balance operational flexibility with legal accountability, ensuring that private entities do not act in ways that inadvertently escalate conflicts or endanger civilian populations.

Corporate governance also plays a critical role in ensuring compliance and accountability. By embedding ethical oversight, board-level security management, and internal compliance mechanisms, private operators can align operational decisions with both legal obligations and international humanitarian principles. Mandatory reporting requirements to state authorities further enhance transparency, allowing regulators to monitor compliance and respond promptly to security breaches. This multi-layered governance approach ensures that private operators are not only technologically secure but also legally and ethically responsible.

The legal frameworks governing dual-use technologies must also be adaptable to emerging threats and technological innovations. As artificial intelligence, autonomous systems, and advanced satellite architectures become increasingly integrated into civilian and military

ISSN: 2582-6433

applications, regulatory standards must evolve to address new vulnerabilities and operational risks. Future regulations should incorporate provisions for periodic review, updates to technical standards, and rapid enforcement mechanisms that account for the dynamic nature of cyber and space-based threats.

In addition to national regulations, international coordination is essential for effective governance of dual-use technologies. Satellites operate across multiple jurisdictions, and cyber operations often have transnational impacts. Harmonizing regulatory standards through treaties, mutual recognition of certifications, and information-sharing mechanisms can reduce gaps in enforcement and ensure consistent application of security measures. International collaboration also facilitates the establishment of compensation frameworks, dispute resolution protocols, and cross-border accountability mechanisms, providing a more resilient global system for managing dual-use technologies.

The integration of security measures, corporate accountability, and international cooperation also contributes to the protection of civilian populations. Dual-use systems increasingly support essential services such as energy, communications, transportation, and financial networks. Ensuring their resilience is not only a matter of national security but also of humanitarian concern. Mandatory regulation, combined with robust oversight and ethical governance, reduces the risk of unintended civilian harm resulting from cyberattacks or operational failures in dual-use systems.

Moreover, implementing mandatory frameworks provides a foundation for future innovation. By establishing clear expectations for security and liability, regulators create an environment where companies can innovate confidently while adhering to enforceable standards. Research and development efforts can focus on enhancing resilience, integrating advanced cybersecurity technologies, and improving operational efficiency, knowing that regulatory requirements are transparent, consistent, and legally binding.

Finally, the evolution of legal frameworks for dual-use technologies is a strategic imperative. In an era of hybrid warfare, cyber-enabled conflict, and rapidly advancing commercial space capabilities, the consequences of unregulated dual-use operations are severe. The combination of legal clarity, enforceable standards, corporate accountability, and international coordination provides a comprehensive approach to mitigate risks, protect critical infrastructure, and maintain global stability. Mandatory regulation represents not only a legal necessity but a strategic tool to align technological advancement with humanitarian, ethical, and security considerations.

ISSN: 2582-6433

In conclusion, the transition from voluntary guidelines to legally binding frameworks is essential to manage the challenges posed by dual-use space and cyber technologies. Case studies such as KA-SAT and Starlink demonstrate both the vulnerabilities of unregulated systems and the potential of private technologies to support strategic objectives. Mandatory regulation ensures consistent security standards, defines liability, promotes corporate accountability, protects civilian infrastructure, and facilitates international coordination. The establishment of enforceable legal frameworks, complemented by robust corporate governance, technical oversight, and ethical review, provides a sustainable model for integrating dual-use technologies into modern conflict environments.

As technology continues to advance, the legal and regulatory structures governing dual-use systems must evolve in tandem. Future frameworks should remain adaptive, incorporating lessons from emerging threats, technological innovation, and operational experiences. By combining enforceable legal standards, corporate responsibility, and international collaboration, the global community can ensure that dual-use technologies serve strategic objectives without compromising security, civilian protection, or ethical obligations. This approach lays the foundation for a secure, accountable, and resilient technological landscape, ensuring that both military and civilian stakeholders can operate with confidence in an increasingly complex and interconnected world.

Future Scope

The legal and regulatory management of dual-use technologies is still an emerging field, and several avenues remain for further research and development:

International Treaty Development: There is a need to explore multilateral treaties that impose enforceable cybersecurity standards for dual-use technologies across national borders. Such treaties could harmonize global obligations, establish dispute resolution mechanisms, and provide frameworks for compensation in cases of cross-border incidents.

Technological Standardization and Certification: Future research can focus on developing standardized technical and operational benchmarks for dual-use space systems, including secure communication protocols, encryption methods, and resilience testing. Internationally recognized certifications could reduce regulatory inconsistencies and enhance global compliance.

Corporate Legal Accountability: Further studies should examine how corporate governance, internal compliance mechanisms, and ethical oversight can be codified into law to ensure accountability for dual-use operations. Research could explore best practices for integrating

ISSN: 2582-6433

corporate responsibility into legal frameworks while preserving innovation and operational flexibility.

Emerging Technologies and AI Integration: As space and cyber infrastructure increasingly rely on artificial intelligence, machine learning, and autonomous systems, legal frameworks must evolve to address the new risks these technologies introduce. Future work should explore the intersection of AI ethics, liability, and cybersecurity law in dual-use systems.

Resilience and Risk Mitigation: Research can also investigate strategies for enhancing the resilience of dual-use technologies, including redundancy, fail-safe mechanisms, and rapid response protocols to minimize the impact of attacks or operational failures. This includes studying the effectiveness of lifecycle-based security measures and post-incident remediation frameworks.

Public Policy and Ethical Implications: Finally, future research should evaluate the broader societal and ethical implications of dual-use technologies, particularly their impact on civilian populations, global equity in access to secure infrastructure, and the potential for misuse in asymmetric conflicts.

By addressing these areas, policymakers, legal scholars, and technology developers can collaboratively create frameworks that balance innovation, operational efficiency, and security. The future of dual-use technologies depends not only on technical advancements but also on robust, enforceable, and ethically grounded legal structures that protect civilians, maintain strategic stability, and promote responsible corporate conduct.

ISSN: 2582-6433

BIBLIOGRAPHY

Books & Journals

1. Duncan B Hollis, 'Cyber Operations and the Use of Force in International Law' (2014) 36 Oxford Journal of Legal Studies 1.
1. Johnson, D. G., & Wetzel, R. (2020). The cyber-space convergence: Legal and strategic implications of dual-use satellite networks. Journal of Strategic Studies, 43(6), 847–872
2. Kremer, J., & Mueller, M. (2019). Cyber-attacks, dual-use space systems, and international humanitarian law: Legal gaps and emerging frameworks. Journal of Space Law, 43(1), 55–88.
3. Moltz, J. C. (2019). Space security and cyber interdependencies: Challenges for global governance. Space Policy, 47, 101–110
4. Johnson-Freese, J. (2017). Space as a strategic domain: State control and military applications. Astropolitics, 15(2), 98–116.
5. Handley, M. (2021). Mega-constellations: Opportunities, challenges, and cybersecurity considerations in modern satellite networks. Journal of Space Safety Engineering, 8(2), 115–127.
6. Handley, M., & Johnson, D. (2022). Economic opportunities and risks in mega-constellation satellite networks. Space Policy, 60
7. Tasdighi, A. (2026). Cyber security for space missions: Mitigating risks in the new space era. Wiley-VCH
8. Shinde, R., & Shinde, V. (2024). Space law, satellite constellation-based internet & cyber security. Barnes & Noble
9. Dale Stephens and Cassandra Steer, 'Conflicts in Space and the Rule of Law' (2015) 39 Journal of Space Law 65.
10. Braw, E. (2023). Private sector power in modern warfare: The role of commercial technology companies in conflict. Survival, 65(2), 7–24.
11. Gleason, M. P. (2022). Satellite mega-constellations and national security implications. Space Policy, 59
12. Johnson, J. (2023). Commercial satellites and the militarization of space. Journal of Strategic Studies, 46(5), 912–934

ISSN: 2582-6433

13. Wright, D. (2022). The strategic implications of satellite mega-constellations. Space Policy, 60
1. Greenberg, A. (2022). The satellite hack everyone missed on the morning Russia invaded Ukraine. Wired. https://www.wired.com
2. https://scientiaeducare.com/mcqs-with-answers-on-the-space-race-a-cold-war-era-competition/
3. Enercon. (2022). Statement on satellite communication disruption affecting wind turbines. https://www.enercon.de