US-China Law Review, February 2025, Vol. 22, No. 2, 79-88
doi:10.17265/1548-6605/2025.02.003

International Legal Framework for Cyber Attacks in Outer Space: The Issue of "Use of Force"

SU Yuting, JIANG Shengli
East China University of Political Science and Law, Shanghai, China

The convergence of outer space and cyber operations has heightened risks of cyberattacks against space infrastructure. Such attacks, marked by non-physicality, cross-domain effects, and anonymity, challenge the prohibition of the "use of force" under Article 2(4) of the UN Charter. This paper examines the legal thresholds for characterizing outer space cyber operations as "use of force" by analyzing the UN Charter, the Tallinn Manual 2.0, and the doctrinal debates on intent, means, and consequences. It critiques the "scale and effects" criterion for inadequately addressing non-physical harms and attribution challenges inherent to cyberattacks. The study advocates for targeted reforms, including the development of specialized rules for outer space cybersecurity, enhanced multilateral cooperation to improve attribution mechanisms and the establishment of binding instruments such as a "Space Cyberattack Defense Convention". These proposals aim to reconcile evolving cyber threats with *jus ad bellum* principles, offering both theoretical and practical pathways to strengthen international law's adaptability to hybrid security threats in the digital and spatial domains.

Keywords: outer space cyberattacks, use of force, UN Charter, Tallinn Manual 2.0, scale and effects, international legal regulation

Introduction

In recent years, outer space exploration has emerged as a pivotal domain for global technological competition and international collaboration. The rapid advancement of outer space technologies has significantly enhanced communication, navigation, scientific research, and commercial applications, while also contributing to the evolution of global governance and economic development. However, the unique physical and legal characteristics of outer space render it highly dependent on the security and stability of cyber infrastructure, making it a critical target for cyber-attacks. Such attacks not only disrupt technological systems but also pose risks of transnational economic losses, security crises, and threats to international peace and stability. As cyber operations extend from terrestrial domains to outer space, their non-physical, cross-domain, and anonymous nature introduces complexities in the application of international law, particularly in determining whether such actions constitute a "use of force"—a pressing legal issue requiring resolution by the international community.

SU Yuting, undergraduate student, research assistant, Institute of International Law and Policy on Global Commons Governance, International Law School, East China University of Political Science and Law, Shanghai, China.
JIANG Shengli, associate professor, director, Institute of International Law and Policy on Global Commons Governance, International Law School, East China University of Political Science and Law, Shanghai, China.

Article 2(4) of the United Nations Charter establishes a clear prohibition on "use of force", providing a foundational legal framework for the international community. Concurrently, the Tallinn Manual 2.0 serves as a critical reference for assessing the application of international law to cyber operations, offering systematic guidance on the legal characterization of cyber-attacks. The divergence in scope and standards between these frameworks creates a basis for analyzing whether cyber operations in outer space constitute a "use of force".

This article employs the constitutive elements of "use of force" as an analytical framework to compare the criteria outlined in the United Nations Charter and the Tallinn Manual 2.0. By integrating the distinctive attributes of outer space cyber operations, it systematically examines their legal characterization under international law. Specifically, the paper analyzes the legal standards for traditional uses of force, identifies parallels and distinctions with outer space cyber operations, and proposes potential solutions within the context of existing legal frameworks.

The Concept of "Use of Force" in International Law

Conceptual Dimensions of "Use of Force"

The term "use of force" serves as a cornerstone concept in international law for restricting warfare and maintaining peace, reflecting the international community's profound shift from recognizing the legality of war to comprehensively prohibiting the use of armed coercion.[1] Under traditional international law, war was long regarded as a legitimate means for states to pursue policy objectives, with relatively lax regulation of hostilities. However, as the scale of conflicts expanded and their catastrophic impacts on international order and human societies became evident, the necessity for stricter regulation of armed actions gained global recognition (Brownlie, 1963; Lesaffer, 2015, p. 35).[2]

The adoption of the United Nations Charter following World War II formally established the prohibition of the use of force.[3] The Preamble of the Charter explicitly states one of its aims as being "to ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used, save in the common interest".[4] Article 2(4) further stipulates that all members "shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations".[5] The *travaux préparatoires* of the Charter reinforce this interpretation: during the San Francisco Conference, the Brazilian delegation's proposal to include "the threat or

---

[1] Judge Jennings took this position in his Dissenting Opinion in the Nicaragua case (Merits), n. 520: "It could hardly be contended that these provisions of the Charter [Articles 2(4) and 51] were merely a codification of the existing customary law. The literature is replete with statements that Article 2, Paragraph 4, for example in speaking of 'force' rather than war, and providing that even a 'threat of force' may be unlawful—represented an important innovation in the law".

[2] For an early comprehensive account of the prohibition of the use of force, see Ian Brownlie, International Law and the Use of Force by States (Clarendon, 1963). For a concise overview of the historical development of the outlawing of war, critiquing the overly simplified treatment of this development by many scholars, see Randall Lesaffer, "Too Much History: From War as Sanction to the Sanctioning of War", in Marc Weller (Ed.), *The Oxford Handbook of the Use of Force in International Law* (Oxford University Press, 2015), p. 35, who argues that the just war tradition continued to influence the law in the modern era and explains how many features of the current jus contra bellum have a basis in this tradition.

[3] Prohibited of war Page 24.

[4] The Preamble of UN Charter Para. 7: "to ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used, save in the common interest".

[5] UN Charter, Art. 2(4).

use of economic measures" within Article 2(4) was explicitly rejected.[6] This underscores the drafters' intent to confine the definition of "force" to armed actions, distinguishing it from economic coercion.[7]

Historically, the conceptualization of "use of force" in Article 2(4) aimed to address the shortcomings of the Covenant of the League of Nations and the Kellogg-Briand Pact (Wolfrum, 2012, p. 45; Corten, 2010, p. 52).[8] The former merely restricted war through procedural requirements (e.g., prohibiting undeclared warfare), while the latter, though aspiring to outlaw war entirely, narrowly defined it as formal interstate armed conflict, failing to regulate other forms of force. The UN Charter replaced the term "war" with the more objective "use of force", yet this concept remains confined to traditional armed actions rather than non-physical measures.[9] This interpretation is corroborated by other Charter provisions: the Preamble's emphasis on "armed force" aligns with Article 42, which authorizes the Security Council to employ "armed force" when necessary to uphold peace, solidifying the Charter's focus on physical coercion.[10]

In summary, Article 2(4) establishes the prohibition of force as a foundational framework for peace in international law. Its core lies in regulating armed actions, not economic coercion or other non-forcible measures. However, evolving security challenges—such as cyberattacks, which may gravely threaten peace despite lacking traditional armed elements—have prompted further legal refinement, exemplified by the Tallinn Manual 2.0's systematic treatment of "use of force" in the digital age.

The Tallinn Manual 2.0 extends the traditional concept of the "use of force" under international law to cyberspace. Rule 68, in conjunction with Article 2(4) of the United Nations Charter, explicitly states that "a cyber operation constituting a threat or use of force against the territorial integrity or political independence of any State, or that is otherwise inconsistent with the purposes of the United Nations, is unlawful".[11] This provision integrates traditional international law with cyber governance, emphasizing that the "use of force" in cyberspace is not limited to physical attacks but encompasses non-physical cyber operations. It thereby broadens the applicability of the prohibition to include a wider range of cyber activities.[12] Furthermore, Rule 68 clarifies that the "use of force" is not restricted to actions by a State's armed forces. Any cyber operation attributable to a State—including those conducted by entities authorized, directed, or controlled by the State—qualifies as a use of force if its nature, consequences, or objectives meet the criteria under international law.[13]

---

[6] UN Doc. 784/I/1/27 (Vol. VI), at 335; UN Doc. 885/I/1/34 (Vol. VI), at 400.

[7] UNCIO, Vol. VI, UN Doc. 748/I/1/27 (5 June 1945), 335. But note, UNCIO, Vol. VI p. 400, UN Doc. 885/I/1/34 (9 June 1945), Report of the Rapporteur of Committee 1 to Commission I, regarding Article 2(4): "The Committee likes it to be stated in view of the Norwegian amendment to the same paragraph that the unilateral use of force or similar coercive measures is not authorized or admitted. The use of arms in legitimate self-defense remains admitted and unimpaired. The use of force, therefore, remains legitimate only to back up the decisions of the Organization at the start of a controversy or during its solution in the way that the Organization itself ordains. The intention of the Norwegian amendment is thus covered by the present text".

[8] See Rüdiger Wolfrum, "Preamble" in Bruno Simma et al. (Eds.), *The Charter of the United Nations: A Commentary* (Oxford University Press, 3rd ed, 2012), Vol. I, p. 45. See Olivier Corten, *The Law Against War: The Prohibition on the Use of Force in Contemporary International Law* (Hart Publishing, 2010), p. 52, Footnote 12 for a list of statements by States in the debates in the UN General Assembly preceding votes on major resolutions on the boundaries of the prohibition, reaffirming that Article 2(4) prohibits all measures "short of war".

[9] Prohibited of war Page 116.

[10] UN Charter, Art. 42.

[11] UN Charter, Art. 2(4); Tallinn Manual 2.0, Rule 68.

[12] See Nicaragua judgment, Para. 191 (distinguishing grave uses of force from lesser forms).

[13] Tallinn Manual 2.0, Rules 15-18 (State responsibility and attribution).

Building on Rule 68, Rule 69 further defines the threshold for characterizing a cyber operation as a use of force. According to Rule 69, "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force".[14] This standard, grounded in the *Nicaragua* judgment's emphasis on "scale and effects"[15], provides a critical framework for assessing equivalence between cyber and traditional uses of force. By focusing on consequential harm rather than the instrument employed, Rule 69 addresses gaps in international law concerning cyberspace and ensures consistency with jus ad bellum principles.[16]

Therefore, Rules 68 and 69 of the Tallinn Manual 2.0 establish a legal framework for evaluating cyber operations as uses of force, anchored in traditional international law while adapting to the unique challenges of cyberspace.

Criteria for Determining "Use of Force"

The question of whether cyber operations constitute a prohibited "use of force" under Article 2(4) of the United Nations Charter has generated significant doctrinal debate among Western international legal scholars. While a consensus acknowledges that cyberattacks may, under certain conditions, qualify as such, divergent interpretations persist regarding the provision's substantive scope and applicability. These disagreements crystallize into three principal theoretical frameworks: the teleological approach, the instrumentalist approach, and the scale and effects criterion.

The teleological approach prioritizes the intent and strategic objectives of the act over its material manifestations. Proponents argue that the determination of "use of force" must account for the actor's purpose and the systemic consequences of the operation, rather than relying exclusively on physical damage thresholds. Walter G. Sharp (1999) critiques traditional physicality-based paradigms as insufficient to address the multidimensional nature of cyber threats. He asserts that even cyber operations lacking immediate kinetic effects—such as those targeting critical infrastructure, governmental decision-making systems, or economic stability—may equate to prohibited force if their strategic aim is to "erode state sovereignty, paralyze military readiness, subvert political institutions, or induce societal collapse" (Sharp, 1999, p. 140). This interpretation aligns with the telos of Article 2(4), which seeks to safeguard the "territorial integrity and political independence" of states against coercive interference, irrespective of the means employed.[17] By emphasizing functional equivalency to conventional armed attacks, this approach provides a legal framework adaptable to evolving technological threats.

In contrast, the instrumentalist approach focuses on the means and technical attributes of cyber operations. Central to this framework is whether the tools or methods employed exhibit characteristics analogous to traditional military weaponry. Marco Roscini (2010) argues that cyber operations constitute "use of force" when their design or deployment mirrors the destructive capacity of conventional arms, or when they create effects traditionally associated with kinetic warfare. This view draws support from the Charter's textual dichotomy: while Article 51 references "armed attack" (armed force), Article 2(4) employs the broader term "force",

[14] Tallinn Manual 2.0, Rule 69.
[15] Nicaragua judgment, Para. 191.
[16] Nuclear Weapons advisory opinion, Para. 39; UN GGE 2013 Report, Para. 19.
[17] UN Charter, Art. 2(4).

suggesting an intentional distinction that accommodates non-kinetic modalities (Roscini, 2010, pp. 94-97).[18] Critics, however, anchor their objections in historical context, noting that the Charter's drafters envisioned "force" as encompassing only physical or mechanical coercion. Subsequent state practice, including the 1970 Friendly Relations Declaration, reinforces this restrictive interpretation by excluding "economic, political, or other forms of pressure" from the definition.[19] Instrumentalists counter that such exclusions do not preclude the classification of cyber operations as force, provided their effects replicate the coercive severity of traditional military action.

The "scale and effects" doctrine, which centers on the actual impact of an action, posits that whether an act constitutes a "use of force" depends on the scale of destruction and the actual effects it produces.[20] The International Court of Justice (ICJ) articulated this standard in the *Nicaragua* case to distinguish between the "use of force" and other forms of intervention. In that case, the provision of weapons and training by the United States to the Nicaraguan "contras" was deemed a "use of force", whereas mere financial support did not meet this threshold.[21] This standard has been further clarified in the Tallinn Manual 2.0, where Rule 69 adopts the "scale and effects" criterion to determine whether a cyber operation constitutes a "use of force".[22] In practice, if a state provides malicious software and related training to an armed group, enabling them to carry out destructive cyber operations, such actions would constitute a "use of force" provided their effects are comparable to those of traditional armed force.

In applying the "scale and effects" doctrine to cyber operations, the Tallinn Manual 2.0 outlines several key factors.[23] Severity is the primary criterion, requiring an evaluation of whether the operation causes substantial harm to critical national interests, particularly in terms of its scope, duration, and intensity. Immediacy concerns the temporal aspect of the consequences; operations that produce immediate effects are deemed more threatening, as they reduce the potential for peaceful dispute resolution. Directness assesses the causal relationship between the action and its consequences: the more direct and clear the link, the more likely the operation will be legally recognized as a use of force. These factors underscore the importance of evaluating the immediacy and directness of consequences to determine the overall threat posed by a cyber operation.

However, the application of these eight factors, derived from the "scale and effects" doctrine, remains subject to scrutiny and refinement. On one hand, the "scale and effects" standard was originally developed within the context of traditional armed attacks, primarily addressing physical destruction. Cyber operations, by contrast, exhibit both physical and non-physical characteristics, with consequences ranging from system malfunctions and data manipulation to information warfare, which are not easily analogous to physical destruction. Consequently, the "scale and effects" standard may not fully encompass the dual nature of cyber operations. Relying on this standard as the primary basis for assessing whether a cyber operation constitutes a "use of force" risks an overemphasis on outcome-based evaluation, potentially leading to subjective disputes. On the other hand, the

---

[18] Analyzing the Charter's drafting history and textual variations between "force" and "armed force".

[19] Declaration on Principles of International Law Concerning Friendly Relations and Co-operation among States, UNGA Res 2625 (XXV) (24 October 1970), Annex, Principle 1.

[20] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge University Press, 2017), Rule 69, pp. 335-336.

[21] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, ICJ Reports 1986, Para. 195.

[22] Tallinn Manual 2.0, supra Note 1, Commentary to Rule 69, Para. 8.

[23] Ibid., Commentary to Rule 69, Paras. 9-16.

international community’s practical experience and case law regarding cyber operations in outer space remain limited, insufficient to thoroughly validate the eight factors outlined in the “scale and effects” doctrine. Disagreements persist among states and international organizations regarding the assessment of factors such as the “breadth of consequences” or “severity”, often constrained by technical limitations and contextual variations.

Returning to the “scale and effects” doctrine itself, as noted above, it essentially extends the framework for evaluating physical destruction, thereby inheriting its inherent limitations in assessing effects with a temporal lag. Cyber operations targeting outer space often produce outcomes that manifest only after a significant delay. For instance, a cyber intrusion into a satellite control system may initially result only in performance degradation rather than total incapacitation. In such cases, an overreliance on outcome-based evaluation could lead to delayed regulatory intervention. Moreover, cyber operations in outer space can simultaneously affect terrestrial, orbital, and spatial domains, rendering a single outcome-based standard inadequate for assessing cross-domain destructive effects.

Therefore, in constructing a legal framework for cyber operations in outer space, it is insufficient to rely solely on the “scale and effects” doctrine and its eight factors. Instead, it is necessary to comprehensively consider the technical characteristics, modalities, and multifaceted consequences of such operations. Building on this foundation, the applicability of the “scale and effects” standard should be continuously tested and refined through the accumulation and analysis of practical case studies. Such dynamic adjustment will ensure that the standard accurately and fairly reflects the legal nature of cyber operations in outer space.

Cyberspace Operations in Outer Space and the Threshold of “Use of Force” in International Law

The distinction between outer space cyberattacks and traditional use of force lies primarily in their methods of execution and the nature of their consequences, despite both having the potential to result in similar outcomes. Traditional use of force is typically defined by direct, overt physical destruction, leading to casualties, damage to infrastructure, and violations of state sovereignty. In contrast, outer space cyberattacks, although not involving physical destruction, can produce equivalent outcomes through the disruption of critical functions or the manipulation of data.

Regarding the immediacy of action, traditional use of force—such as military invasions or missile strikes—tends to be immediate and manifest, with a clear causal relationship between the act and its consequences. For instance, a missile strike leads to the destruction of infrastructure or loss of life, establishing a direct connection between the act and the resulting damage. In contrast, outer space cyberattacks are more indirect, relying on sophisticated technical means such as jamming communication links, infiltrating ground control stations, or altering system parameters. The covert nature and technical complexity of these attacks obscure the direct causal chain between the act and its ultimate effect. For example, the 2011 U.S. Congressional report highlighted cyberattacks on the Landsat-7 satellite between 2007 and 2008, in which attackers attempted to alter the satellite’s orbit by disrupting its ground control systems (U.S.-China Economic and Security Review Commission, 2011, pp. 215-217). Although the attack failed, the potential consequences included the satellite losing control, possibly colliding with other objects in orbit and causing significant damage to the space environment. These indirect consequences complicate the causal link between the cyberattack and its ultimate outcomes.

In terms of scale and effects, traditional use of force is typically associated with immediate and widespread physical destruction, such as the collapse of infrastructure or the disruption of social order. While outer space cyberattacks may not result in direct physical damage, they can still lead to severe or even more far-reaching consequences through the incapacitation of critical systems. For example, cyberattacks on communication or navigation satellites could simultaneously disrupt global logistics, financial transactions, and military operations. The 2019 Galileo satellite outage, officially attributed to a technical malfunction, serves as an example of the potential scale of such disruptions (Global Times, 2019). Had it been caused by a cyberattack, the consequences could have been catastrophic across multiple vital sectors. This cross-sectoral impact suggests that outer space cyberattacks could exceed the damage typically associated with traditional use of force, underlining their potentially extensive and devastating effects.

Finally, attribution remains a significant challenge. Traditional use of force generally involves clear perpetrators, such as national armed forces or state-backed non-state actors, whose actions are typically traceable to specific orders and consequences. In contrast, outer space cyberattacks are often difficult to attribute due to their covert nature, the distributed execution of the attacks, and the technical complexity involved. A notable example is the 2018 Russian “proximity operations” case, in which Russia was accused of attempting to intercept data from a U.S. communication satellite (BBC, 2018). Despite the allegations, the covert nature of the operation and the lack of physical damage made it difficult to establish clear attribution and legal responsibility. The use of multiple nodes, third-party servers, or relay satellites to obscure the origin of the attack further complicates efforts to hold perpetrators accountable under international law.

Current Status and Enhancement of International Legal Regulation of Outer Space Cyberattacks

Current Status of International Legal Regulation

The non-physical nature, cross-domain consequences, and complexity of outer space cyberattacks present significant challenges to the existing international legal framework. International law, which has primarily focused on regulating traditional uses of force, lacks clear definitions and standards for addressing emerging threats such as cyberattacks. This gap highlights the need for further development in areas such as responsibility attribution and regulatory frameworks. Disagreements persist within the academic community regarding whether existing legal norms should be applied to cyberspace or whether new frameworks should be created to specifically address cyberattacks.

The complexity of responsibility attribution is further compounded by the diverse nature of outer space cyberattacks, which include direct intrusions into satellite systems and interference with ground stations and communication links. For instance, during the 2020 launch of Iran’s Jamaran-1 communications satellite, an alleged cyberattack targeted the ground station, aiming to alter orbital data by disrupting the control chain (BBC, 2020). This incident underscores how outer space cyberattacks have expanded to affect the entire space activity chain. The extensive use of spoofing technology in cyberattacks has caused significant disruptions in global transportation and posed considerable threats to regional security and economic stability. A case in point occurred in 2017, when multiple vessels in the Persian Gulf were diverted due to spoofed signals (The Washington Post,

2017). The challenge of attribution only intensifies the complexity of legal regulation, as both technical and legal obstacles hinder the identification of perpetrators. Although the consequences of these cyberattacks meet the threshold for “use of force”, establishing accountability remains a significant challenge.

Moreover, the current legal framework reveals substantial gaps in regulating outer space cyberattacks. While core instruments like the Outer Space Treaty establish fundamental principles for the peaceful use of outer space, they do not address non-traditional threats such as cyberattacks. Although the Tallinn Manual 2.0 offers preliminary legal analysis of cyberattacks, it is based on existing customary international law, extending these norms to cyberspace rather than establishing new legal standards. As a non-binding guideline, the Tallinn Manual 2.0 does not possess the authority of binding international law. Overall, international legal frameworks governing outer space cybersecurity remain underdeveloped, with unclear definitions, insufficient standards for identifying cyberattacks, and a lack of mechanisms for responsibility allocation. Additionally, there is no comprehensive system for addressing the consequences of cyberattacks or for determining responsibility among states involved in space-related activities.

Pathways for Enhancing International Legal Regulation

Achieving consensus on the regulation of outer space cybersecurity is a fundamental prerequisite for strengthening the rule of law in both outer space and cyberspace. The enhancement of the international legal framework for outer space cyberattacks requires a multifaceted approach, incorporating rulemaking, responsibility attribution, and international cooperation.

First, the international community should prioritize the establishment of specific rules to address outer space cyberattacks, thereby clarifying the application of existing principles. In 2013, Russia introduced the concept of “cybersecurity in space activities” during the UN discussions on the Long-Term Sustainability (LTS) Guidelines, proposing a draft guideline prohibiting attacks or interference with foreign ground space facilities (Committee on the Peaceful Uses of Outer Space, 2013). This initiative prompted significant international attention to the issue of outer space cybersecurity. In the 2016 LTS negotiations, both the United States and Russia presented draft guidelines to enhance the security and resilience of ground facilities essential to space systems and prevent cyberattacks on foreign space hardware and software. These proposals represent valuable steps toward refining the regulatory framework for outer space cybersecurity.

Expanding the concept of “force” to include cyber disruptions, interference, and falsification of space assets is a necessary and justifiable step, particularly when such actions pose significant risks to global economic stability and international peace. Additionally, the obligation of “due regard” must be emphasized, requiring states to respect the security of foreign ground information infrastructure, uphold jurisdiction over space assets such as satellites, and refrain from malicious use of ICTs that could harm space objects and related systems.

Second, addressing the attribution issue is crucial in regulating outer space cyberattacks. Technological advancements present viable solutions, such as blockchain for real-time tracking of attack paths, encryption to ensure the integrity of data, and artificial intelligence to improve attribution accuracy. However, no single state possesses the capacity to comprehensively address attribution independently, highlighting the need for international collaboration. A multilateral “Outer Space Cyberattack Identification Center” could be established to integrate the technical resources and legal expertise of multiple states, facilitating the traceability of

cyberattacks and the equitable allocation of legal responsibility. Sharing satellite data, technical documents, and attack path analyses would enhance the ability to identify perpetrators and improve attribution accuracy, thereby increasing the effectiveness of legal regulation.

Finally, international cooperation is indispensable. Drawing from the EU's regional cybersecurity initiative following the Galileo system incident, a global framework for defending against outer space cyberattacks is urgently needed. Regional cooperation mechanisms, such as the Asia-Pacific Space Cooperation Organization, should be leveraged to promote collaboration and technology sharing in the defense against such attacks. On the international level, the establishment of a "Space Cyberattack Defense Convention" should be considered. This convention should clearly define "outer space cyberattacks", distinguishing them from traditional physical attacks and establishing standards for evaluating non-physical consequences. Additionally, the convention should create a unified model for responsibility allocation in the event of cyberattacks in outer space cooperation projects, introducing shared responsibility clauses to enhance project stability and address cross-border incidents. The convention should also encourage multinational technological cooperation, enabling states to share resources and data, regularly releasing technical evaluations, and establishing a "Global Cyberattack Traceability Database" to improve attribution efficiency.

The rise of cyber operations in outer space presents significant challenges to the established framework of international law, exposing gaps and delays in the legal response to rapidly advancing technology. This article examines the legal implications of the "use of force" as defined in the United Nations Charter and the Tallinn Manual 2.0, considering the complex, cross-domain nature of cyber operations in space. It identifies key shortcomings in the international legal system, particularly in areas such as attribution, responsibility allocation, and regulatory standards, and proposes potential solutions through rule refinement, international cooperation, and technological innovation. However, this study is limited by the scarcity of empirical data and the lack of practical case law. Future research will require the development of case studies to facilitate the integration of theory and practice, ultimately achieving more effective and precise legal regulation of outer space cyber operations to ensure international peace and security.

References

BBC. (2018). U.S. alerts on Russian satellite's "anomalous activities" raising concerns. Retrieved from https://www.bbc.com/zhongwen/simp/chinese-news-45211036

BBC. (2020). Analysis of cyber interference in Iran's communication satellite launch. Retrieved from https://www.bbc.com/news/world-middle-east-53908256

Brownlie, I. (1963). *International law and the use of force by states*. Oxford: Clarendon Press.

Committee on the Peaceful Uses of Outer Space. (2013). Long-term sustainability of outer space activities. 2024-02-271. A/AC.105/C.1/L.337.

Corten, O. (2010). *The law against war: The prohibition on the use of force in contemporary international law*. Glidden: Hart Publishing.

Global Times. (2019). Galileo system outage: Exposing vulnerabilities of global satellite navigation infrastructure. Retrieved from https://opinion.huanqiu.com/article/9CaKrnKlR3X

Lesaffer, R. (2015). Too much history: From war as sanction to the sanctioning of war. In M. Weller (Ed.), *The Oxford handbook of the use of force in international law* (p. 35). Oxford: Oxford University Press.

Roscini, M. (2010). Worldwide warfare—*Jus ad Bellum* and the use of cyber force. *Max Planck Yearbook of United Nations Law, 14*, 102-105.

Sharp, W. G. (1999). *Cyberspace and the use of force.* Alexandria: Aegis Research Corporation.

The Washington Post. (2017). Report on GPS spoofing and signal jamming incident in the Persian Gulf. Retrieved from https://www.washingtonpost.com/gps-spoofing-gulf-incident-analysis

U.S.-China Economic and Security Review Commission. (2011). Chapter 3: Section 2: China's Cyber Activities Directed against the U.S. Government and Military. In *2011 annual report to congress* (pp. 215-217). New York: U.S.-China Economic and Security Review Commission.

Wolfrum, R. (2012). Preamble. In B. Simma et al. (Eds.), *The charter of the United Nations: A commentary* (Vol. I, 3rd ed., p. 45). Oxford: Oxford University Press.