Adv. J. Manag. Humanit. Soc. Sci. (2026), Volume 2, Issue 4, 368-379

Advanced Journal of Management, Humanity and Social Science

Journal homepage: https://www.ajmhss.com/

DOI: https://doi.org/10.5281/zenodo.22954827

International Responsibility of States for Cyberattacks against Peaceful Space Facilities in Light of the United Nations Charter

Hassan Bagheri[1*], Anita Yousefi[2]

[1]PhD Candidate in Public International Law, Teaching Assistant at Islamic Azad University, Karaj Branch, Karaj, Iran

[2]PhD Candidate in Public International Law, Teaching Assistant at Islamic Azad University, Karaj Branch, Karaj, Iran

Article info

Received: 25.06.2026

Accepted: 25.09.2026

Available Online: 25.09.2026

Checked for Plagiarism: Yes

Keywords:

State Responsibility; Space Cybersecurity; Peaceful space Facilities; United Nations Charter

ABSTRACT

Peaceful space facilities constitute an interdependent terrestrial-orbital infrastructure: satellites, ground stations, mission-control networks, user terminals, inter-satellite links, and software-dependent services. A malicious cyber operation directed at any one of these components may disrupt essential civilian functions far beyond the immediate target. Yet a damaging cyber incident does not itself establish an internationally wrongful act of a state, and an internationally wrongful act does not necessarily constitute a prohibited use of force or an armed attack. This article develops a sequential doctrinal framework for evaluating state responsibility for cyber operations against peaceful space facilities under the United Nations Charter, the 1967 Outer Space Treaty, and the law of state responsibility. Its method is qualitative legal analysis of primary instruments, current United Nations materials and peer-reviewed scholarship published principally in 2024-2026, supplemented by carefully labelled hypothetical scenarios. It distinguishes technical attribution, legal attribution, the content and breach of primary obligations, injury and reparation, and the independent conditions for lawful responses. It argues that article III of the Outer Space Treaty confirms the applicability of the Charter in the space domain, whereas articles VI-IX add distinctive but non-identical obligations concerning national space activities, launch-related liability, jurisdiction and control, and due regard. These rules should not be collapsed into a blanket presumption that a state is responsible for every cyberattack by a private actor connected to its territory. An effects-sensitive analysis can identify conduct potentially falling under article 2(4), while the more demanding armed-attack inquiry governing article 51 requires a separate assessment of scale, effects, necessity and proportionality. The proposed evidentiary and institutional approach prioritizes timely incident preservation, reasoned legal attribution, consultations and reversible non-forcible measures. It addresses the legal uncertainty surrounding non-destructive interference, due diligence and the reach of the specialized space-liability regime without treating contested interpretations as settled law.

Introduction

Modern civilian dependence on satellite communications, positioning and timing, Earth observation, meteorological services, disaster response and scientific missions has made peaceful space infrastructure an attractive target for malicious cyber operations. An adversary need not physically approach a spacecraft to affect its function. Compromise of a software update, command key, gateway router or control workstation may interrupt services, misdirect a platform, corrupt telemetry or undermine the integrity of data upon which other institutions rely. The European Union Agency for Cybersecurity (ENISA) describes the satellite lifecycle as an interconnected attack surface encompassing development, deployment, operation and decommissioning [5,6].

These technical dependencies matter legally because one operation can involve infrastructure, operators, beneficiaries and harmful effects across several

Corresponding Author: **Hassan Bagheri (hasangsmal@gmail.com)*

2 Email: mrsyousefi77@gmail.com

jurisdictions. The central legal question is narrower than whether cyber threats to space systems are serious. It is when a specific act or omission involving a state, established by persuasive evidence and measured against a particular international obligation, engages international responsibility. That inquiry must distinguish a malfunction from a hostile operation; conduct attributable to a state from activity merely traceable to computers in its territory; breach of a primary rule from the secondary consequences of breach; and the mere occurrence of harmful effects from the much higher threshold for an armed attack. The conceptual discipline is important both for victim states seeking remedies and for states accused on insufficient evidence [1-4].

This article addresses five questions. What counts as a peaceful space facility and which regulatory regimes apply to its terrestrial and orbital components? How a cyber operation attributed to a state without converting technical indicators into conclusive legal proof? Which obligations breached below, at, and above the threshold of a prohibited use of force? How do the Charter and the Outer Space Treaty interact, particularly concerning national private activities and damage? Finally, which measures are legally available to the affected state? The article answers these questions through a sequential test rather than by assuming that all attacks on peaceful infrastructure have the same legal characterization.

The temporal scope is deliberate. The analysis draws on the 2024 study by Bace, Gökce and Tatar, the 2024 study by Li, the 2024 UNIDIR legal primer, the 2025 ENISA space threat landscape, the 2025 final report of the UN open-ended working group on information and communication technologies, and a 2026 UNIDIR space-security report [1-8]. Foundational treaties, the International Law Commission (ILC) Articles on State Responsibility, and leading judgments necessarily predate this three-year research window: they cited as continuing primary legal authorities, not misrepresented as newly published research [9-13]. The cutoff for this review is 24 September 2026.

Research Design, Scope and Terminology

Doctrinal method and limits

This is a qualitative doctrinal inquiry, not a quantitative estimate of cyber incidents or a claim to identify perpetrators of any real-world incident. Primary rules extracted from treaty texts and accepted legal instruments; their interaction tested against recent scholarship and institutional reports. Where the law is unsettled, the article identifies competing interpretations and specifies the facts on which legal conclusions depend. Four wholly hypothetical scenarios used to demonstrate how the same event can lead to different outcomes depending on attribution, the protected interest, severity and the foreseeability of collateral effects. No empirical frequencies, fabricated interview findings or numerical security scores inferred from those scenarios.

Three distinctions govern the method. First, internationally wrongful conduct requires both legal attribution and violation of a binding obligation, irrespective of the political desirability of the conduct [11]. Second, technical evidence of an operation and legal responsibility for that operation concern different propositions: ownership of a server, malware-language clues or IP geolocation rarely resolves whether a state organ acted or whether private actors followed state instructions. Third, conduct causing loss may engage a sector-specific compensation regime without independently proving a breach of the Charter. The conclusion reached under one branch not used as a substitute for the elements of another.

Meaning of a peaceful space facility

For analytical purposes, a "peaceful space facility" is a satellite, scientific instrument, orbital platform, spacecraft-support function or essential terrestrial digital/physical component predominantly used for civil, scientific, commercial or humanitarian space activity. The term is functional rather than a novel treaty category. It includes command-and-control ground stations, telemetry tracking systems, launch-support computers, communications gateways, user terminals, mission data centres and cloud-based operational software. A satellite may serve mixed civilian and military clients, and a nominally civilian facility may provide services later used by armed forces; therefore, purpose, actual use and legal status must be assessed rather than inferred from an operator's commercial name [5,6].

"Cyberattack" used descriptively to mean an intentional hostile operation employing information and communication systems to disrupt, manipulate, deny or damage a space-related component or its services. This working term does not predetermine the narrower meanings of an "attack" under international humanitarian law, an "armed attack" under Article 51, or a "use of force" under Article 2(4). Jamming and spoofing may be electronically mediated without identical technical pathways to software intrusions; they are considered only insofar as they illuminate the legal consequences of interference with space-linked information or commands [1,5].

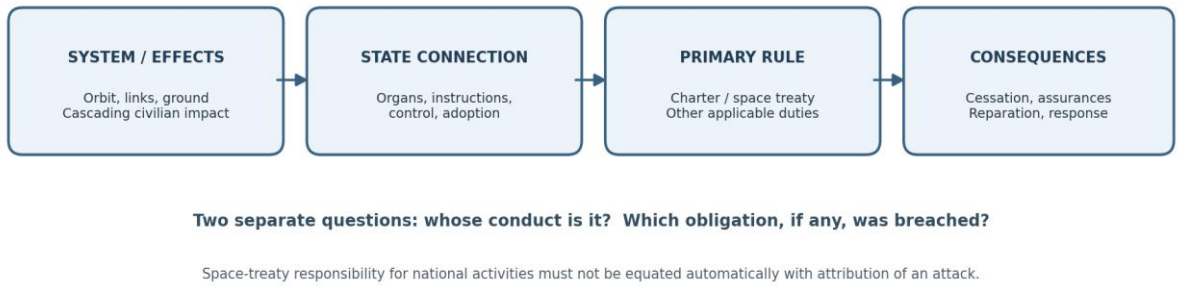

Figure 1. Analytical sequence for classifying space-related cyber incidents. Original schematic; arrows indicate legal questions, not a presumption of responsibility.

The Applicable Normative Framework

The Charter applies to space and cyber activity

Article 2(4) of the United Nations Charter requires members to refrain from the threat or use of force in their international relations against the territorial integrity or political independence of any state, or in any other manner inconsistent with United Nations purposes. Article 51 recognizes the inherent right of individual or collective self-defense if an armed attack occurs, subject to its conditions and the Security Council framework. Article 33 provides a menu of peaceful dispute-settlement methods, and the Council has responsibility for the maintenance of international peace and security [9]. Nothing in those provisions confines relevant conduct to kinetic weapons or terrestrial locations. The UNIDIR 2024 primer specifically examines the applicability of the prohibition on force in outer space and highlights unresolved threshold questions [3].

The proposition that the Charter applies to state conduct involving information and communication technologies has been reaffirmed in the UN's intergovernmental cyber-security process. The final report transmitted in 2025 under A/80/257 records consensus work concerning responsible state behaviour, international law, confidence-building, capacity-building and institutional dialogue [7]. Consensus on applicability does not erase divergence over how sovereignty, due diligence, intervention, countermeasures and the level of force should be understood in a given case. Analysis must therefore be article-specific, not based on an assertion that a new free-standing "space cyber law" already supplies every answer [1,2,7].

Space treaties: integration without doctrinal collapse

Article III of the 1967 Outer Space Treaty directs states parties to carry on activities in the exploration and use of outer space in accordance with international law, including the Charter, with regard to international peace, security and cooperation. Article I protects freedom of exploration and use; Article II bars national appropriation. Article VI makes states parties internationally responsible for national activities in outer space, whether carried on by governmental agencies or non-governmental entities, and requires authorization and continuing supervision of the latter. Article VII addresses international liability of specified launching states for damage caused by their space objects. Article VIII gives the state of registry jurisdiction and control over the registered space object, while Article IX requires due regard for corresponding interests and contemplates consultations in relation to potentially harmful interference [10].

Those provisions have different triggers and purposes. Article VI concerns national space activities and ensuring compliance with the Treaty; its application to an independently operating private cyber attacker, as opposed to a licensed operator's own space operations, raises questions about the scope of "national activities in outer space." Article VII attaches to a launching-state relationship and damage caused by the space object; it is not a generic strict-liability rule for every remotely delivered digital harm. Article VIII is a jurisdictional hook and may support the identification of the relevant regulatory state, but it does not make every unauthorized intrusion attributable to that state. Article IX may bear on prevention and consultation even when Article 2(4) is not implicated, though the precise content of ex ante cyber precautions remains context-dependent [2,10].

The 1972 Liability Convention elaborates a specialized compensation structure: absolute liability for damage caused by a space object on the surface of Earth or to aircraft in flight and fault-based liability for certain damage elsewhere, with treaty-defined concepts and claims procedures [12]. Whether remote data corruption, loss of service or an indirect terrestrial economic loss counts as damage "caused by" a space object is contestable and fact-specific. In particular, the characterization of a malicious cyber command as an act by the space object itself should not be assumed. The general rules of state responsibility may remain relevant if an independently binding obligation was breached,

but the availability of a separate lex specialis remedy requires careful examination.

General responsibility and interaction of legal regimes

The ILC Articles on Responsibility of States for Internationally Wrongful Acts (ARSIWA) organize the secondary rules: conduct attributable to a state and breach of an international obligation (Article 2), conduct of state organs (Article 4), conduct of persons exercising elements of governmental authority (Article 5), direction or control (Article 8), and acknowledgement and adoption of conduct as the state's own (Article 11). Articles 30–31 address cessation, non-repetition in appropriate circumstances and full reparation; Articles 34–37 distinguish restitution, compensation and satisfaction. Articles 49-53 govern countermeasures by injured states and preserve important limits, including that countermeasures may not involve the threat or use of force [11].

ARSIWA does not create an all-purpose primary obligation to prevent each cyber incident. Nor does the phrase "international responsibility" in Article VI of the Outer Space Treaty automatically reproduce the general attribution tests in every factual setting. A more defensible reading asks first whether the relevant conduct is a national space activity governed by a specific treaty obligation; if not, ordinary attribution rules govern the alleged interstate cyber operation, together with any independently applicable due-diligence, sovereignty or non-intervention obligation. A state may accordingly incur responsibility for its own regulatory failure without automatically owning the private attacker's distinct conduct [2,10,11].

Table 1. Distinct legal routes and their analytical thresholds.

Legal route	Required inquiry	Potential result / limit
ARSIWA Articles 2, 4, 8, 11	Attributable act or omission + breach of a primary duty	State responsibility; intrusion infrastructure alone is not decisive.
UN Charter Article 2(4)	Attributable conduct qualifying as threat or use of force	Prohibition may apply without a kinetic weapon.
UN Charter Article 51	An armed attack plus necessity/proportionality and other conditions	Self-defence is not triggered by every unlawful cyber operation.
Outer Space Treaty Article VI	National activity in outer space; compliance, authorization, supervision	Treaty responsibility differs from automatic attribution of any private intrusion.
Outer Space Treaty Articles VII-IX	Launching-state damage; registered object; due regard/consultation	Distinct relationships, duties and remedial pathways.
1972 Liability Convention	Treaty-defined damage caused by space object + location/fault rules	Coverage of pure digital or consequential loss remains disputed.

Attribution: From Forensic Indicators to State Conduct

Technical, legal and public attribution

Attribution operates at three levels. Technical attribution seeks to identify attack pathways, infrastructure, malware and human operators. Legal attribution tests whether proved conduct can be treated as an act of a state under rules such as ARSIWA Articles 4, 5, 8 or 11. Public or political attribution is the decision to name an actor and may rely on intelligence that cannot be disclosed. They overlap but are not interchangeable. Li's 2024 analysis of malicious cyber activities against space activities emphasizes the importance of differing operational roles of the affected space systems and the limits of both general and space-specific attribution approaches [2].

A ground gateway operated by a corporation in State A may relay malicious packets originating from a compromised third-country machine; the satellite may be registered by State B and offer civilian services in States C and D. None of these facts, individually, shows that State A or B directed the attack. Technological methods such as log correlation, cryptographic signing, telemetry verification, endpoint imaging and independent network evidence can establish a stronger chain of events. Relevant nontechnical evidence might include authenticated communications, evidence of official tasking, institutional control, or a state's express adoption of the specific operation as its own. The quality and provenance of proof matter more than a single marker such as an IP address [1,2,5].

The main legal gateways

Conduct of a ministry, military unit or intelligence service acting as a state organ is ordinarily attributable under Article 4 even if the organ exceeds domestic authority, subject to the applicable conditions. A private company empowered to exercise governmental authority may fall under Article 5 when acting in that governmental capacity;

being commercially important or state-licensed alone does not satisfy this description. Conduct by an external group may be attributable under Article 8 where the necessary instructions, direction or control over the conduct are shown, while Article 11 concerns a state's acknowledgement and adoption of the conduct as its own. The tests should be applied to the relevant operation rather than to generalized political sympathy or the mere existence of a cooperative relationship [11].

The evidentiary burden is particularly demanding where the harmful consequences are cross-domain and the attacker can exploit commercial hardware and geographically dispersed cloud infrastructure. An investigator might establish that a spacecraft acted on falsified commands while remaining unable to establish who created them. Conversely, evidence may convincingly identify a state organ's unauthorized access to a command network, yet the documented effects may be limited to surveillance rather than interference. These records can support different primary-rule analyses, and an unproved attribution claim cannot be repaired by overstating the gravity of the outcome [1,2].

Omission and the contested due-diligence route

A distinct possibility concerns a state's failure to act after credible warning that infrastructure or an operator within its jurisdiction is being used to cause serious harm. The extent of a generally binding duty to prevent malicious cyber operations by non-state actors, and its precise standard, remain debated. A prudent analysis identifies the alleged primary duty, its source, the knowledge attributable to the state, the feasibility of protective steps and a causal connection to any claimed loss, rather than treating due diligence as universally settled and outcome-guaranteeing. A licensing and supervision failure under Article VI may provide a more specific route where the actors and activities fall within that provision [2,7,10].

Due regard under Article IX supplies an additional treaty-based lens for states parties conducting their own space activities. A state planning a cyber-relevant change to a spacecraft that foreseeably creates potentially harmful interference with another state's activity should examine the applicable duty of consultation. Whether a state that does not operate the interfering object must monitor every cross-border cyber route is a different question. In neither case does an eventual outage alone retrospectively prove that every ex-ante precaution was legally required or technically feasible [10].

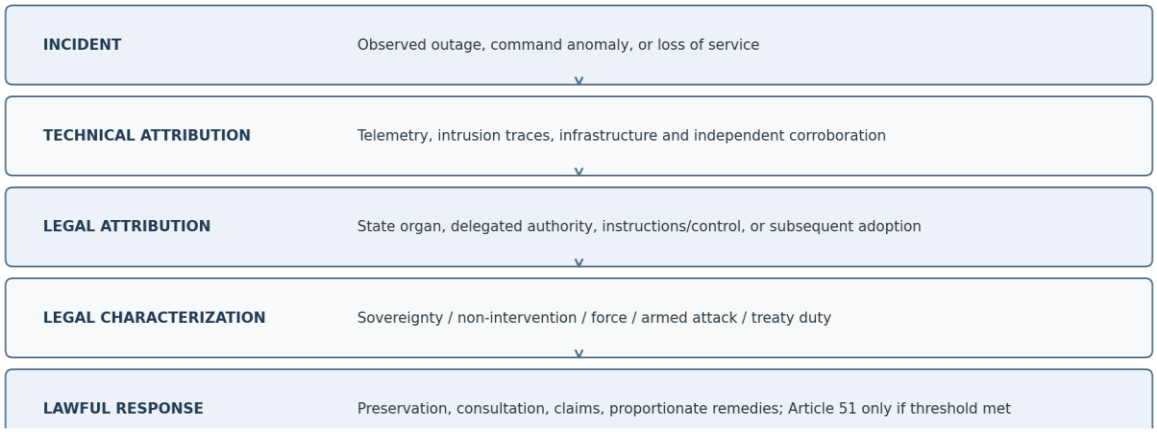

Figure 2. Evidence-to-response workflow. Original schematic separating factual reconstruction, attribution, legal characterization and permissible measures.

Identifying the Breached Primary Obligation

Sovereignty, non-intervention and protected functions

Compromise of a state-controlled ground station physically situated in its territory may raise sovereignty concerns even if no component is destroyed. However, states and scholars disagree about whether sovereignty supplies a stand-alone prohibition for every remote cyber intrusion and, if so, the precise threshold of infringement. A reasoned claim should therefore specify whether the intrusion caused physical effects, functional loss, interference with inherently governmental operations or another legally cognizable violation, and should distinguish treaty-based duties from contested broader formulations. The fact that outer space itself is not subject to national appropriation under Article II does not mean that ground facilities lose the territorial protection afforded by international law [1,3,10].

The rule of non-intervention requires analysis of coercion in a domain in which the target state is legally entitled to decide freely. An operation that disables a civilian satellite in order to compel a state to alter its external policy presents a different legal claim from espionage, commercial criminality or

short-lived unauthorized access without that coercive component. Motive cannot be inferred solely from interruption. Demonstrable communications, coordinated demands, timing and the mechanism by which the victim's decision-making was constrained may be legally material. The protected civilian character of the facility is relevant context, not a substitute for proving coercion [1,7].

Article 2(4): assessing uses of force

An attributable operation that causes a space object to collide with another object, destroys a platform, or leads to extensive physical damage on Earth can raise an especially serious Article 2(4) question. In less tangible settings long-duration denial of navigation, corruption of emergency-weather data, or interference with hospital-linked satellite communications the legal assessment is less settled. Effects, scale, directness, immediacy, duration, reversibility and the relationship to traditional forms of force may inform analysis; none is a universally agreed numerical test. UNIDIR's 2024 primer treats outer-space applications of the Charter prohibition as legally relevant while stressing unresolved interpretive issues [3].

A narrow view associates the use-of-force prohibition principally with physical injury or damage comparable to kinetic conduct. An effects-oriented approach holds that severe, predictable disruption of essential civilian functions may qualify even if the attacker uses only code and no hardware is destroyed. These are not necessarily mutually exclusive across all scenarios: the stronger the physical and operational consequences, the easier the comparison; purely economic or brief service losses leave wider disagreement. This article does not propose that each cyber intrusion into a satellite is force. The legal conclusion must address intensity and consequences on the proved facts, not rely on the rhetorical designation of a service as "critical" [1,3,7].

Moreover, Article 2(4) concerns interstate force and has to be linked to state conduct under the appropriate attribution rules. It is insufficient that a commercial operator suffers large losses, that the incident is technically sophisticated, or that public commentary labels it a hostile state operation. The place where consequences appear may differ from the place where code was introduced; in a multi-state service network, identifying the affected states and the interstate dimension requires detailed factual mapping. The Outer Space Treaty confirms, rather than replaces, the Charter's relevance in this domain [3,9,10].

Article 51: the independent armed-attack inquiry

The Charter distinguishes a prohibited use of force from the occurrence of an armed attack capable of triggering Article 51, a distinction developed in the International Court of Justice Nicaragua judgment [13]. A cyber operation should not be described as an armed attack merely because it violates sovereignty, disables a satellite or merits reparations. An armed-attack analysis evaluates the scale and effects of the incident, including reasonably established and causally connected human or physical consequences, while acknowledging uncertainty concerning severe non-physical disruption. The question of whether a series of related operations can be assessed together also requires evidence of operational connection and legal justification, not simply temporal proximity [3, 9].

Even when the armed-attack threshold is met, a state invoking self-defense must satisfy necessity and proportionality, comply with the Charter's reporting framework, and consider the particular risks of any proposed response to civilian and third-state space systems. A response aimed at stopping an attack cannot be justified by a generalized desire to punish its author. Where attribution remains unresolved, an irreversible forcible response risks imposing grave consequences on the wrong state or on innocent operators. This problem is acute in satellite networks whose shared services support users across borders [3,5,9].

The survival of a spacecraft after a malicious command does not settle the legal question in either direction. Consider two hypothetical extremes: (a) a recoverable interruption of a weather-data portal with no demonstrated consequences for safety, and (b) deliberate manipulation of collision-avoidance commands that causes a high-energy impact and foreseeable casualties or substantial physical destruction. The different consequences, attributable conduct and any evidence of an ongoing attack would require separate analysis. Between them lie serious service-denial cases for which state practice and legal opinion remain insufficiently uniform to justify a categorical formula [1,3].

Table 2. Illustrative distinction among possible legal characterizations (not a ranking or empirical scale).

Illustrative effects	Question requiring proof	Cautious legal treatment
Transient unauthorized access, no service loss	Whose act? Which confidentiality or territorial interest?	Wrongfulness depends on a particular duty; force cannot be presumed.
Repeated disruption of a state emergency ground station	Attribution, territorial/functional impact, coercion	Possible sovereignty or intervention issue; Article 2(4) requires separate analysis.

Extended loss of essential satellite-dependent services	Scale, civilian consequences, directness and duration	Potential force question; absent agreement on non-physical thresholds.
Spoofed command leads to destructive spacecraft collision	Causation, state conduct, physical impact and magnitude	Strong Article 2(4) question; assess armed attack independently.
Attack causes widespread destruction and loss of life	Verified causal chain, severity, necessity of proposed response	May engage Article 51 if all conditions are met; not an automatic licence for retaliation.

The Special Position of Peaceful, Private and Dual-Use Facilities

Peaceful purpose is not immunity from every hostile act

Space systems that provide civil services are particularly valuable to global welfare; however, "peaceful" is not a single immunity provision in the Charter or Outer Space Treaty that automatically resolves all cyber operations. Article IV of the Outer Space Treaty regulates particular military uses and weapons-related activities, especially weapons of mass destruction in orbit and activities on celestial bodies, but does not categorically prohibit every military support function performed by a satellite. A civilian service may be contracted by a military end-user without transforming every linked device into a lawful target, and the legal regime applicable during armed conflict has requirements distinct from the peacetime Charter inquiry [10].

Where an armed conflict exists, international humanitarian law raises further questions about distinction, proportionality, precautions and the status of dual-use objects. Those questions demand facts concerning the parties, the existence and classification of conflict, the relevant military use and foreseeable civilian harm. The present article does not attempt to decide such cases or treat commercial ownership as a universal legal shield. It focuses on peacetime state responsibility while noting that the Charter's rules on resort to force and humanitarian rules on conduct during conflict must not be conflated [1,3].

Private operators and supervisory states

Commercial operators may control satellites serving foreign governments, and national authorities may authorize and supervise the enterprise under Article VI of the Outer Space Treaty. Regulatory responsibilities can include risk-based licensing conditions, security auditing, incident reporting and continuing review where these measures are warranted by the treaty and relevant national implementation. The scope of Article VI should be assessed in relation to the operator's national outer-space activity: it is not a treaty shortcut for attributing every activity of a criminal gang using a satellite terminal, nor does a regulator become an international guarantor against all hacking [2,5,10].

The 2025 ENISA space threat landscape highlights cyber weaknesses arising from third-party components, legacy technology, limited remote visibility and human error, and frames controls across the whole satellite lifecycle [5]. Such technical findings can inform what reasonable operational supervision may entail but cannot independently create a universal international legal standard. An authorization decision may be negligent under domestic law without necessarily breaching an international obligation; conversely, an operator can comply with local checklists yet be involved in internationally wrongful state conduct if a governmental agency directs its offensive actions. Careful separation of public regulation, operator duties and governmental direction avoids both over-attribution and accountability gaps [2,5,11].

Multiple states and international organizations

A single mission may involve a state of registry, one or more launching states, a state granting commercial authorization, a foreign ground-station host and a state whose nationals rely on the service. Their legal interests and potential duties are not identical. Article VIII links jurisdiction and control to registration; Article VII and the Liability Convention involve launching-state relationships; Article VI ties responsibility to national space activities and has a separate clause concerning activities of international organizations [10,12]. As a result, one state may be best placed to preserve telemetry, another to inspect a compromised terminal, and a third to present an injury claim. Their practical capacity to investigate does not by itself establish responsibility for the attack.

If an international organization operates the system, the allocation of the organization's own conduct and the duties of participating states must be analyzed on the relevant instruments and facts. Joint missions also pose disclosure and privilege issues in evidence sharing. The appropriate investigative strategy is therefore cooperative but not indiscriminate: preserve secure logs, establish lawful information-sharing channels, document custody of technical material and distinguish public incident reporting from material needed to prove an international legal claim [2,8,10].

Four Hypothetical Case Analyses

The following scenarios are constructed solely to stress-test legal propositions; they describe no particular historical incident or finding against any

actual state. They deliberately vary the proof of state involvement and the effects of the same broad class of operation. The point is to identify missing facts that would change an outcome, not to attach an automatic legal label to a technology.

Case A: private ransomware at a mission-data centre

A criminal group encrypts non-operational files at a scientific mission's data centre in State A and demands payment. A state-funded astronomy platform remains safely controlled; researchers lose access to data for five days. Forensic investigators find that commands passed through compromised hosts in State B, but no evidence connects the group to its government. State A could seek criminal-law cooperation, preservation of evidence and assistance through applicable arrangements. International responsibility of State B for the group's conduct cannot be inferred from routing alone. A claim based on omission would need a separately supported duty, relevant notice, available measures and breach. Nor should the incident automatically be termed a use of force simply because science is interrupted [1,2,11].

Case B: state-organ manipulation of Earth-observation outputs

An authenticated operational record and official tasking documents show that a state intelligence unit inserts false flood images into a foreign space agency's emergency-response feed. No spacecraft is physically harmed, but the manipulated data materially affects evacuation decisions. Article 4 attribution is much clearer than in Case A. The legal analysis must then identify the injured state's protected interests, any proven interference with governmental functions, the foreseeability and actuality of harm, and whether the conduct is coercive within the non-intervention rule. The severe downstream human consequences, if reliably established, are relevant to force analysis; data falsification alone does not mechanically determine the Article 2(4) or Article 51 classification [1,3,11].

Case C: licensed operator's unpatched command gateway

A private satellite operator licensed in State A repeatedly ignores documented critical warnings about its gateway despite a national supervisory authority's knowledge that multiple spacecraft depend on that component. Unknown outsiders compromise the system and temporarily deny emergency communications in several states. The identity of the outside attackers remains unproven. The regulator's actions or omissions require examination under relevant authorization and continuing-supervision obligations if the gateway is integral to national space activity. The attackers' conduct should not be attributed to State A merely because the company is licensed there. Any civil damages, treaty liability, Article IX due-regard claim and ARSIWA reparation claim would require their own predicates and proof of causation [2,5,10-12].

Case D: spoofed collision-avoidance instruction

Authenticated records show that a military cyber unit of State A knowingly injects false commands into State B's registered civilian satellite, causing a collision that destroys the spacecraft and threatens nearby objects. State-organ attribution is assumed proved for the hypothesis. Article 2(4), Article III of the Outer Space Treaty and obligations protecting the other state's space operations require serious examination, as do Article IX due regard and the possibility of compensation under applicable damage rules. Whether the magnitude of the destruction constitutes an armed attack is a distinct question; the need for defensive force cannot be inferred from the fact that physical destruction already occurred. If the launch-related treaty regime is invoked, the claimant must identify a relevant launching state and damage caused by a space object, rather than presuming State A's cyber operation itself satisfies those terms [3,9-12].

Table 3. Hypothetical application: what must be established before choosing a legal route.

Scenario	Attribution status	Most relevant unresolved issue
A. Criminal ransomware	Only hostile non-state activity established	Independent duty and breach by an identified state, if any.
B. Falsified observation data	State organ assumed established	Protected interest, coercion, causal harm and force threshold.
C. Licensed operator's gateway	Operator and regulator known; attacker unknown	Scope of Article VI supervision, breach and causation.
D. Destructive false command	State organ assumed established	Scale/effects, independent Article 51 inquiry and specialized damages path.

Remedies, Response Measures and Institutional Cooperation

Cessation, assurances, reparation

Where a wrongful act is attributable and an international obligation is breached, the responsible state may be required to cease continuing conduct, offer appropriate assurances or guarantees of non-repetition in the circumstances, and make full reparation for injury caused by the wrongful act [11]. For a space cyber operation, restitution might include return of unlawfully obtained control credentials, restoration of compromised operational data or technical assistance in restoring lawful control provided such measures are possible and lawful. Compensation raises difficult proof issues where damages include lost service, physical repair, satellite replacement, mitigation expenditure and consequential losses borne in multiple countries. Satisfaction may be relevant where restitution and compensation alone do not address established injury [11].

A sound claims file should separately document attribution, obligation, wrongful conduct, injury and causation. Data provenance and method are essential: system logs may be overwritten, telemetry may have different clocks, and an operator's own emergency shutdown may contribute to the duration of an outage. For losses stemming from simultaneous network failures, claimants should distinguish harm caused by the attributed operation from unrelated failures. The most persuasive legal submission is not the one with the broadest estimate of harm but the one with transparent assumptions and reproducible evidence [2,5,11].

Retorsion and countermeasures

Lawful but unfriendly acts, commonly termed retorsion, may include diplomatic protest, lawful suspension of voluntary cooperation, or public technical warnings consistent with other obligations. Non-forcible countermeasures are conceptually different because they would otherwise breach a legal obligation but may be justified under strict conditions in response to a prior internationally wrongful act. Under ARSIWA, their purpose must be to induce compliance, they are generally available to an injured state, and they are subject to requirements including proportionality, temporariness where feasible, procedural conditions and protection of specified obligations [11]. The treatment of measures taken by non-injured states remains a separate and contested question; rhetorical claims of collective digital retaliation do not resolve it. No countermeasure may involve the threat or use of force contrary to the Charter. Nor should a victim state infer a carte blanche to compromise unrelated civilian satellites merely because its own services have been interrupted. A disabling response against a shared commercial constellation could foreseeably affect hospitals, aircraft navigation and humanitarian communications beyond the responsible actor. State practice and applicable law warrant preference for measures that are legally characterized, necessary for their permissible purpose, proportionate and reversible where possible. An Article 51 response requires the independent armed-attack conditions already discussed [3,9,11].

Consultation, notification and preservation

Article IX of the Outer Space Treaty supplies a specific consultation setting for activities and experiments that may cause potentially harmful interference with another state party's peaceful exploration or use of outer space. Its precise trigger should not be converted into a compulsory universal pre-incident notice for all cybersecurity events, yet it underscores a cooperative practice relevant to high-risk maneuvers, changes to command systems and mitigation of foreseeable effects. Channels between national space authorities, computer security incident response teams, foreign ministries and commercial operators can reduce uncertainty without requiring premature public legal attribution [7,8,10].

The 2025 UN OEWG report and accompanying international process emphasize international law, confidence-building and institutional dialogue in ICT security [7]. Space-sector practice can build on this by establishing secure 24-hour incident contacts, compatible log-retention protocols, authenticated emergency command procedures and protected technical exchanges after outages. An independent technical investigation can clarify mechanisms even when legal attribution remains unresolved. None of these measures, by itself, constitutes a new binding treaty rule; each can support compliance with existing obligations and prevent escalation from mistaken attribution [5-8].

A practicable evidence-and-response protocol

An affected operator should first isolate compromised channels in a way that avoids endangering spacecraft or other orbital users; record the timeline of commands and subsequent spacecraft behavior; preserve cryptographic, network and command logs with documented custody; and identify operational, contractual and cross-border dependencies. The public authority should then review what can lawfully be shared with the relevant state of registry, launching state, licensing state and affected service users. Only after the facts are sufficiently established should it choose a legal theory and possible response. A state's communication can express uncertainty explicitly, separating a technical finding from a provisional claim about state involvement [2,5,10].

For an operation with imminent risk of collision or severe civilian harm, technical coordination cannot await perfect legal certainty. Operators can take

safety-preserving steps under their existing authorities while state representatives use urgent consultations and evidence-sharing channels. Later claims of wrongful conduct should be grounded in the known record as supplemented by inquiry. This approach avoids two false choices: treating uncertainty as a reason to ignore ongoing danger or treating danger as a reason to dispense with attribution and the legal conditions for responsive force [3,8,10,11].

Table 4. Evidence, legal question and institution in a space-cyber incident.

Operational record or fact	Legal significance	Potential custodian / cooperation route
Signed command logs; satellite telemetry; orbit data	Mechanism, timing, causation, damage and prevention	Operator, state of registry, collision-avoidance networks
Gateway images; malware samples; traffic correlation	Technical actor hypotheses; not sufficient alone for Article 8	CERT/CSIRT, independent forensic specialists, host state
Official tasking; authenticated instructions; adoption statement	Possible ARSIWA Article 4, 8 or 11 attributions	Competent state bodies and lawful intergovernmental exchange
Licensing conditions; audit reports; warning notices	Existence and content of Article VI supervisory obligations	Licensing authority and authorized private operator
Service maps; emergency logs; casualty or repair records	Consequences, injury, causation and threshold analysis	Affected agencies, public-service providers, claims experts
Notice of potentially harmful interference; meeting records	Article IX consultation and risk-reduction practice	National space authorities, diplomatic channels

Discussion: A Layered Model of International Responsibility

The combined doctrinal analysis supports a layered rather than an all-or-nothing model. The first layer describes the system architecture and the operation's actual or reasonably foreseeable effects. The second reconstructs the evidentiary path from a malicious instruction to a legally attributable actor. The third identifies the primary international rule governing the specific conduct, whether a Charter prohibition, a particular space-treaty obligation or another applicable rule. The fourth identifies the secondary consequences and lawful remedies. The model prevents the common error of treating an important victim or a dramatic technical method as a substitute for proof of state conduct and breach [1-3,11].

A distinctive feature of space activity is that different states may occupy legally significant roles without having committed the cyber operation. Registry, launch, licensing and location each open a different set of legal questions. They can identify who must cooperate in evidence preservation and safety measures, while the identities of the perpetrating state, an injured state and a state potentially liable under a specialized space treaty may diverge. This multiplicity makes causal and jurisdictional mapping indispensable. It also cautions against invoking a specialized regime based solely on the fact that a satellite appears somewhere in the chain of harm [2,10,12].

The model also resolves a false dichotomy between a narrow physical-damage rule and unrestricted effects-based classification. For some incidents, physical destruction and human injury supply comparatively clear legal analogies. For non-destructive interference, loss of control, service denial and data manipulation require more finely grained evidence of scale, duration, directness and the protected interests affected. The proper consequence of uncertainty is neither automatic exculpation nor automatic escalation. States can articulate why a particular duty applies, which facts remain unresolved, and what non-forcible measures are justified on the existing record [1,3,7].

Recent institutional developments provide a framework for confidence-building without erasing legal disagreement. The UN General Assembly's 2024 resolution on reducing space threats addresses norms, rules and principles of responsible behaviours [14]. The 2025 cyber OEWG final report reflects the continuation of common work on international law and cooperative measures [7]. The 2026 UNIDIR conference report records discussion among states and other stakeholders on contemporary space-security concerns [8]. These materials can inform interpretation and practice, but a political report or voluntary recommendation must not be equated with a universally binding new prohibition absent an independent legal basis.

Recommendations for Legal Clarification and Operational Practice

First, states should publish carefully qualified views on how Article 2(4) and Article 51 apply to loss of control of a spacecraft, extensive non-physical deprivation of essential satellite services and foreseeable cross-border cascading effects. Such statements should identify considerations and examples without pretending that a fixed global numerical threshold already exists. Publication can make practice more transparent and reduce incentives to relabel routine cyber incidents as armed attacks. The underlying Charter commitments

and the Outer Space Treaty's integration clause remain the legal starting points [3,7,9,10].

Second, regulators can specify risk-sensitive cybersecurity responsibilities for licensed commercial space operators, including credible incident notification, authenticated command pathways, secure supplier management, recovery testing and appropriate oversight of remote ground systems. The normative source and territorial reach of every requirement should be identified. ENISA's 2024 and 2025 sectoral reports offer engineering-oriented inputs, not self-executing international obligations. Article VI compliance should be assessed against the particular state's treaty commitment and the activity under supervision, with recognition that no security system can guarantee zero incidents [5,6,10].

Third, governments and private operators should agree on interoperable technical preservation practices that serve later legal analysis: synchronized telemetry, protected audit trails, command provenance, secure sharing with the registry and licensing states, and procedures for distinguishing safety responses from attacker-caused damage. A joint technical account need not establish the ultimate legal actor, but it can narrow disputes over event chronology and causation. Clear retention and disclosure rules may also help protect confidential communications and sensitive mission information [2,5,8].

Fourth, claims and responses should be tailored. A state advancing an Article VII or Liability Convention claim should identify the space object, relevant launching state, treaty-covered damage and the rule applicable to the place of injury. A state alleging an internationally wrongful cyber operation should specify the attributed conduct and breached primary obligation. A state contemplating an otherwise unlawful countermeasure should separately assess the conditions and limits of ARSIWA; forcible self-defense must be justified, if at all, on the independent Article 51 route. These are cumulative quality controls, not bureaucratic obstacles [9-12].

Finally, multilateral discussions can target remaining doctrinal ambiguity rather than assume it away. Priority subjects include an operational definition of potentially harmful cyber interference for Article IX consultations, evidentiary good practices for public attribution, the extent of preventive duties related to privately operated space systems, and treatment of non-physical loss in compensation claims. A staged process of shared incident terminology, voluntary technical cooperation and transparent legal positions could facilitate future agreements while preserving the distinction between existing law and proposed development [2,7,8,14].

Conclusion

Cyber operations against peaceful space facilities can engage state responsibility under existing international law. The United Nations Charter applies to outer-space activity, as Article III of the Outer Space Treaty expressly confirms, and some cyber operations may implicate the prohibition on force. But the legal analysis turns on demonstrated state conduct, identification and breach of a primary rule, and the actual character and consequences of the operation. The more demanding condition of an armed attack must be evaluated separately before Article 51 can be invoked. Commercial ownership, peaceful purpose, technical sophistication and serious social harm do not dispense with any of those elements [1-3, 9-11].

The space-law provisions add differentiated responsibilities rather than a universal short cut: Article VI concerns national space activity and supervision, Articles VII and the Liability Convention concern particular damage and launching-state connections, Article VIII concerns registry-linked jurisdiction and control, and Article IX addresses due regard and consultations. The proposed layered model treats each route according to its own legal prerequisites. It also acknowledges continuing disagreement over non-physical force thresholds, cyberspace sovereignty, due diligence and the reach of specialized space-damage remedies. The most defensible near-term approach combines technical preservation, rigorous attribution, transparent treaty analysis, cooperative risk reduction and remedies proportionate to established wrongfulness rather than to speculation [2,3,5,7,10-12].

Disclosure Statement

No potential conflict of interest reported by the authors.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Authors' Contributions

All authors contributed to data analysis, drafting, and revising of the paper and agreed to be responsible for all the aspects of this work.

References

[1] Research literature and recent institutional materials (**2024-2026**); foundational primary legal sources are identified separately below. URLs and DOIs are provided to facilitate verification. Access date: 24 September **2026**.

[2] Bace, B., Gökce, Y., & Tatar, U. (**2024**). Law in orbit: International legal perspectives on cyberattacks targeting space systems. Telecommunications Policy, 48(4), 102739.

[3] Li, D. (**2024**). Legal challenges of attributing malicious cyber activities against space activities. Leiden Journal of International Law, 37(4), 963-982.
[4] Pobjie, E., & Azcárate Ortega, A. (**2024**). Outer Space and Use of Force (Space Security Legal Primer 1). United Nations Institute for Disarmament Research.
[5] Azcárate Ortega, A., & Erickson, S. (**2024**). OEWG on Reducing Space Threats: Recap Report. United Nations Institute for Disarmament Research.
[6] European Union Agency for Cybersecurity (ENISA). (**2025**). ENISA Space Threat Landscape 2025.
[7] European Union Agency for Cybersecurity (ENISA). (**2024**). Low Earth Orbit (LEO) SATCOM Cybersecurity Assessment.
[8] United Nations General Assembly. (**2025**). Developments in the field of information and telecommunications in the context of international security: Final report of the Open-ended Working Group on Security of and in the Use of ICTs 2021-2025 (A/80/257, 24 July 2025).
[9] Mai, C., & Mathe, T. (**2026**). Outer Space Security Conference 2025 Report. United Nations Institute for Disarmament Research.
[10] United Nations. (1945). Charter of the United Nations, especially Articles 2(3)- (4), 33, 39-42 and 51.
[11] United Nations. (**1967**). Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, especially Articles I-IV and VI-IX.
[12] International Law Commission. (**2001**). Draft Articles on Responsibility of States for Internationally Wrongful Acts, with commentaries. Yearbook of the International Law Commission, vol. II, part two.
[13] United Nations. (**1972**). Convention on International Liability for Damage Caused by Space Objects.
[14] International Court of Justice. (**1986**). Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, I.C.J. Reports 1986, p.14.
[15] United Nations General Assembly. (**2024**). Reducing space threats through norms, rules and principles of responsible behaviors (A/RES/79/22, adopted 2 December 2024).