BRIDGING NORMS OF RESPONSIBLE BEHAVIOR: FROM CYBERSPACE TO OUTER SPACE GOVERNANCE

Ulpia Elena BOTEZATU
National Institute for Research and Development in Informatics – ICI Bucharest, Romania
Romanian Space Agency
ulpia.botezatu@ici.ro, ulpia.botezatu@rosa.ro

Abstract: The increasing integration of digital and space infrastructures makes cross-domain governance more than an intellectual analogy: it creates an operational requirement. This article examines which elements of the international framework for responsible State behaviour in the use of information and communications technologies can be adapted to outer space security without obscuring the legal, physical and institutional differences between the two domains. It conducts a structured, focused qualitative comparison of United Nations cyber norms, Organization for Security and Co-operation in Europe confidence-building measures, the space transparency and confidence-building acquis, the Outer Space Treaty, the Guidelines for the Long-term Sustainability of Outer Space Activities, relevant technical standards and selected operational practices. Transfer is assessed against five criteria: functional equivalence, legal compatibility, observability, institutional feasibility and control of unintended effects. The analysis finds that the most promising transfers are not substantive prohibitions copied from one domain to another, but governance design patterns: policy transparency, validated points of contact, protected crisis communications, tiered incident reporting, cooperative assistance, capacity-building and implementation by the actors best placed to manage risk. Three case studies—the political commitment not to conduct destructive direct-ascent anti-satellite missile tests, the 2022 KA-SAT cyberattack and conjunction assessment and coordination—demonstrate both the value and the limits of this approach. The article proposes a phased, measurable roadmap that reinforces existing space law and institutions rather than replacing them. Its central claim is that cyber diplomacy offers outer space governance a method for turning broad expectations into repeatable practice; the content and legal basis of each measure must nevertheless remain space-specific.
Keywords: responsible behaviour; cyber norms; outer space governance; international law; space security; confidence-building measures; satellite cybersecurity; capacity-building.

INTRODUCTION

The outer space environment is simultaneously congested, contested, and commercially vibrant. The rising density of objects in key orbits, the growing role of dual-use capabilities and the dependence of terrestrial societies on satellite services create multiple pathways for accidents, misperception and escalation. Space-enabled positioning, navigation and timing, communications, Earth observation, meteorology and financial synchronisation have become embedded in national critical infrastructures. At the same time, space systems depend on terrestrial networks, cloud services, supply chains and software. The operational boundary between space security and cybersecurity is therefore porous even though the two fields remain institutionally and legally distinct.

In cyberspace, governments have spent over a decade articulating voluntary, non-binding norms of responsible State behaviour and building practical confidence-building measures

(CBMs) intended to enhance predictability. The resulting framework is imperfect, and its implementation remains uneven. It nevertheless demonstrates how diplomacy can move from general principles to recurring practices: national-policy publication, networks of policy and technical points of contact, requests for assistance, incident cooperation, responsible vulnerability reporting and capacity-building. These mechanisms do not eliminate conflict. Their more modest and realistic purpose is to reduce avoidable uncertainty, open channels before a crisis and distribute implementation responsibilities among States, operators and technical communities.

The central argument of this article is that selected cyber norms and CBMs are transferable to outer space—not as a one-to-one transplant, but as governance design patterns that can be adapted to orbital realities and the existing space law acquis. This distinction is essential. A cyber measure cannot be presumed suitable merely because a space system contains digital components. Nor should cyber terminology be used to bypass unresolved questions in space security. Transfer is justified only where a cyber practice performs a comparable risk-reduction function, can be anchored in applicable space law and policy, produces sufficiently observable conduct, can be implemented by a legitimate institution and does not create disproportionate security or commercial costs.

The research question addressed by this article is therefore: Which cyber-derived practices can strengthen behaviour-based outer space security, under what legal and institutional conditions, and with which safeguards? The article makes three contributions. First, it situates the proposed transfer within the pre-existing space transparency and confidence-building acquis, including the 2013 report of the Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities and the 2023 recommendations of the United Nations Disarmament Commission (UNGA, 2013b; UNDC, 2023). Second, it develops an explicit transfer test rather than relying on superficial similarity. Third, it converts the comparison into an implementation roadmap that identifies responsible actors, appropriate sequencing and measurable indicators.

The analysis proceeds as follows. Section 2 explains the method and limitations. Sections 3 and 4 examine the cyber and space governance baselines. Section 5 compares the two domains. Section 6 maps selected cyber design patterns into space practice. Section 7 tests the framework against three cases. Sections 8 and 9 address legal and institutional implications and propose a phased roadmap. The conclusion identifies the conditions under which voluntary behaviour can become operationally meaningful.

This article develops and substantially expands preliminary findings presented at the 76th International Astronautical Congress (IAC 2025). The present version adds an explicit methodology, incorporates the space TCBM acquis, differentiates legal obligations from political commitments and technical standards, develops comparative case studies, and provides a measurable implementation framework.

METHODOLOGY AND ANALYTICAL FRAMEWORK

The article uses structured, focused comparison. It does not treat cyberspace and outer space as equivalent strategic environments. Instead, it compares the governance functions performed by selected measures in each domain. The source corpus is purposive and consists primarily

of official instruments and implementation documents produced between 2013 and July 2026. For cyberspace, it includes the consensus reports of the UN Groups of Governmental Experts (GGE), the reports of the UN Open-ended Working Groups (OEWG), General Assembly endorsements, OSCE CBM decisions and operational guidance for non-State stakeholders. For outer space, it includes the Outer Space Treaty, the COPUOS Long-term Sustainability (LTS) Guidelines, the UN space TCBM reports, General Assembly processes on reducing space threats, the political commitment against conducting destructive direct-ascent anti-satellite missile tests, relevant International Telecommunication Union (ITU) rules and selected technical standards.

Official documents are prioritised because the article evaluates what States and institutions have actually accepted, recommended or operationalised. Expert manuals and scholarly literature are used for interpretation, not as substitutes for State consent or treaty law. The Tallinn Manual 2.0 and the Woomera Manual are therefore treated as non-binding expert works that organise legal arguments; neither is presented as an independent source of law (Schmitt, 2017; Beard and Stephens, 2024).

The comparison is functional rather than terminological. A "point of contact", for example, is not transferred because the same phrase appears in both domains. It is assessed because a validated route to an authorised official can reduce delay, authenticate communications and prevent technical anomalies from being interpreted as hostile acts. Similarly, "incident response" is examined not as a universal formula, but as a set of decisions about notification, evidence preservation, confidentiality, assistance and recovery that may be adapted to space-system anomalies.

Each proposed design pattern is evaluated against five criteria:

1. Functional equivalence - Does the measure address a substantially similar governance failure, such as uncertainty about intent, lack of an authorised contact or fragmented incident evidence?
2. Legal compatibility - Can the measure operate consistently with applicable treaty duties, national jurisdiction, commercial confidentiality, data-protection obligations and security restrictions?
3. Observability - Can relevant actors identify implementation through credible indicators without demanding disclosure that would create unacceptable vulnerabilities?
4. Institutional feasibility - Is there an institution with an appropriate mandate, membership, expertise and decision-making practice to facilitate the measure?
5. Unintended-effects control - Could the measure generate false reassurance, enable intelligence collection, expose proprietary information, impose unequal costs or shift responsibility away from actors capable of preventing harm?

Treating transfer as adaptation rather than replication is consistent with policy-transfer research, which shows that incomplete, uninformed or context-insensitive transfer may produce policy failure (Dolowitz and Marsh, 2000). It is also consistent with scholarship on the construction of cyber norms, which emphasises that the effects of a norm depend not only

on its wording, but also on the actors involved, the processes through which it is articulated and the practices through which it is implemented and contested (Finnemore and Hollis, 2016).

The test is deliberately demanding. A measure may be useful but still fail as a global norm if it cannot be observed or if no suitable institution can administer it. Conversely, a highly observable practice may be legally or strategically unacceptable. The framework therefore supports modular adoption: States may begin with national implementation, test interoperability in regional or like-minded settings and move towards broader arrangements when evidence of utility exists.

The analysis focuses primarily on peacetime risk reduction and crisis management. The KA-SAT cyberattack is used as a boundary case to identify lessons concerning resilience, cross-border coordination and incident response under hostile conditions; the article does not examine the application of the law governing the use of force or international humanitarian law to that incident.

Nor does the article claim that repeated voluntary conduct has already generated customary international law. The identification of a rule of customary international law requires sufficiently general State practice accepted as law, or opinio juris; the repetition of political commitments alone is insufficient (ILC, 2018).

Public evidence also imposes limits. Cyber attribution may depend on classified intelligence, while precise satellite manoeuvre plans, telemetry and command architectures may be commercially sensitive or security-classified. The proposed measures consequently rely on tiered disclosure, authenticated channels and minimum-necessary data.

The three cases were selected to test different dimensions of the framework. The commitment concerning destructive direct-ascent anti-satellite missile tests examines a narrowly defined and relatively observable restraint measure. The KA-SAT incident tests cross-domain dependence, attribution constraints and resilience under hostile conditions. Conjunction assessment examines a mature safety practice that already performs functions associated with confidence-building. The cases are therefore analytically diverse illustrations rather than statistically representative samples; their purpose is to test mechanisms and expose boundary conditions, not to establish universal causal effects.

NORM DEVELOPMENT AND IMPLEMENTATION IN CYBERSPACE

The UN framework of responsible State behaviour

The contemporary UN cyber-stability framework combines the applicability of international law, eleven voluntary, non-binding norms of responsible State behaviour, confidence-building measures and capacity-building. The 2013 GGE reached consensus that international law, particularly the Charter of the United Nations, applies to State conduct involving information and communications technologies (ICTs) (UNGA, 2013a). The 2015 GGE consolidated the eleven norms and related recommendations, including the protection of critical infrastructure, appropriate responses to requests for assistance, ICT supply-chain integrity, responsible reporting of ICT vulnerabilities and the expectation that States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs (UNGA, 2015). The

General Assembly subsequently welcomed the report and called upon Member States to be guided by it, giving the framework universal political visibility (UNGA, 2015a).

The 2021 GGE did not create a new list of norms. Its principal added value was implementation guidance that clarified possible national measures and forms of cooperation (UNGA, 2021a). The parallel OEWG broadened participation to all Member States and reinforced the integrated character of the framework: rules and norms are more credible when accompanied by CBMs, assistance and institutional capacity (UNGA, 2021b). The 2021–2025 OEWG continued this work and produced its final report in document A/80/257 (UNGA, 2025). General Assembly resolution 80/16 then established a permanent Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs (UNGA, 2025a). The institutional form has changed, but the core lesson remains stable: implementation requires recurring procedures rather than periodic declarations.

Three features of this acquis matter for outer space. First, the norms are framed as expectations of responsible behaviour, allowing risk reduction even where States disagree about new legally binding rules. Second, implementation is distributed. Governments are indispensable, but infrastructure owners, vendors, computer-security incident-response teams, researchers and civil society perform many of the actions that make the norms real. Third, capacity-building is not an optional development supplement. Without trained personnel, legal authorities, secure communications and incident-management capability, formal agreement produces unequal and fragile implementation.

The OSCE model: confidence through practice

The OSCE translated broad cyber-stability objectives into a regional catalogue of CBMs through Permanent Council Decisions No. 1106 of 2013 and No. 1202 of 2016 (OSCE, 2013; OSCE, 2016). The measures cover voluntary information exchange, national terminology, points of contact, consultations, protection of critical infrastructure and secure communication channels. They do not require States to reveal operational capabilities. Their value lies instead in creating habits of contact and a common procedural vocabulary before an emergency.

Several design choices are especially relevant. The OSCE separates policy and technical functions rather than assuming that one contact can resolve every problem. It encourages exchanges about national organisation and terminology, which reduces avoidable ambiguity. It also connects points of contact to protected communication arrangements. A directory without validation, duty procedures or an authentication mechanism is merely an address book; a functioning CBM requires regular testing, updated roles and the authority to escalate a message.

The OSCE model also illustrates that CBM performance is cumulative. A single notification rarely creates trust. Repeated meetings, exercises and responses allow participants to assess whether counterparts are reachable, whether terminology is understood and whether escalation routes work. This operational conception of confidence is more useful for space governance than an abstract expectation that transparency automatically produces benign intentions.

From State norms to multistakeholder implementation

The Geneva Manual on Responsible Behaviour in Cyberspace demonstrates a second implementation pathway: unpacking State-endorsed norms into roles for non-State stakeholders. Its first chapter addresses ICT supply-chain security and responsible vulnerability reporting; the second develops critical-infrastructure protection (Kazakova, Radunović and Droz, 2023; Geneva Dialogue, 2025). The Manual has no law-making status. Its importance lies in showing how a broad norm can be decomposed into actors, actions, dependencies and unresolved questions.

Comparable operational mechanisms include national and sectoral computer-security incident-response teams, vulnerability-disclosure policies, information-sharing communities and sector-specific exercises. These mechanisms work when incentives and safeguards are credible. Operators will not disclose a vulnerability if notification predictably produces disproportionate liability, public exposure or loss of sensitive intellectual property. States will not use a crisis channel if its messages cannot be authenticated. Consequently, effective norm implementation combines an expectation of conduct with procedures governing confidentiality, data minimisation, response time and escalation.

This point corrects a common misconception about voluntary norms. Their weakness is not simply the absence of legal enforceability. A legally non-binding measure can influence procurement, licensing, insurance, professional practice and reputation. Conversely, a broadly supported norm may remain inert when responsibilities, costs and evidence are undefined. The question for outer space is therefore not whether cyber norms are "binding enough", but whether selected implementation architectures can make existing space obligations and commitments more predictable in practice.

THE OUTER-SPACE GOVERNANCE BASELINE

Treaty law and regulatory responsibility

Outer-space governance begins with treaty law, not with borrowed cyber concepts. Article III of the 1967 Outer Space Treaty places space activities within the wider framework of international law and the Charter of the United Nations. Article VI establishes international responsibility for national activities in outer space, including activities conducted by non-governmental entities, and requires their authorisation and continuing supervision by the appropriate State. Article IX requires due regard to the corresponding interests of other States Parties and provides for consultations where an activity or experiment would cause potentially harmful interference. Article XI supports information-sharing concerning the nature, conduct, locations and results of space activities, subject to feasibility and practicability (United Nations, 1967).

These provisions supply more precise legal anchors than a generic appeal to "due diligence". Due diligence remains useful as an analytical description of reasonable, risk-sensitive conduct, but its exact status and content are contested across legal contexts. In concrete space governance, authorisation and continuing supervision under Article VI, due regard and consultations under Article IX, and applicable ITU obligations concerning harmful interference provide firmer points of attachment. National licensing can translate these responsibilities into

operator requirements for cybersecurity governance, contact availability, anomaly reporting, collision avoidance and post-mission disposal.

Radio-frequency coordination adds a specialised legal and technical layer. Article 45 of the ITU Constitution requires stations to be established and operated so as not to cause harmful interference to the radio services or communications of other Member States and recognised operating agencies that function in accordance with the Radio Regulations (ITU, 2023; ITU, 2024). Cyber interference, radio-frequency interference and physical interference should not be collapsed into one category. They may produce similar service degradation but differ in evidence, applicable rules, competent institutions and appropriate remedies.

Safety and long-term sustainability

In 2019, COPUOS adopted by consensus 21 Guidelines for the Long-term Sustainability of Outer Space Activities, which were subsequently welcomed by the General Assembly. The Guidelines address regulatory frameworks, the safety of space operations, international cooperation, capacity-building and scientific and technical research (COPUOS, 2019; UNOOSA, 2021). Guideline A.1 concerns national regulatory frameworks, while Guideline A.3 addresses the supervision of national space activities. Guidelines B.1 to B.5 address updated contact information, the accuracy and sharing of orbital data, conjunction assessment during all orbital phases of controlled flight and practical approaches to pre-launch conjunction assessment. Section C addresses international cooperation, capacity-building and awareness.

Cybersecurity is increasingly integrated into space-system engineering. Space Policy Directive-5 articulates risk-based cybersecurity principles across spacecraft, ground-control and user networks (United States, 2020). NISTIR 8401 applies the NIST Cybersecurity Framework to commercial satellite operations, including ground systems, command and control, protection, detection, response and recovery (Lightman et al., 2022). ISO/TS 20517:2024 provides requirements and recommendations for cybersecurity management across space systems, including spacecraft, launchers, payloads and ground equipment (ISO, 2024). These instruments are not interchangeable: national policy, implementation guidance and international technical specifications have different authority and audiences.

The existing space TCBM and responsible-behaviour acquis

Any proposal to adapt cyber CBMs must recognise that outer space already has a substantial transparency and confidence-building lineage. The 2013 GGE report on TCBMs in outer space recommended exchanges of information on national space policies and activities, risk-reduction notifications, consultations, exchanges of contact information, visits to space facilities, international cooperation and coordination (UNGA, 2013b). In 2023, the United Nations Disarmament Commission adopted by consensus recommendations to promote the practical implementation of those measures, including through national reporting, information exchanges, notifications and strengthened coordination (UNDC, 2023). Existing research has similarly emphasised that norms can provide flexible and incremental forms of risk reduction, while remaining subject to challenges concerning scope, interpretation, participation and political legitimacy (West and Azcárate Ortega, 2022).

The responsible-behaviour process added a more explicitly security-focused vocabulary. General Assembly resolution 75/36 invited States to identify existing and potential threats and

to share views concerning responsible and irresponsible behaviour (UNGA, 2020). Resolution 76/231 established an OEWG on reducing space threats through norms, rules and principles of responsible behaviours (UNGA, 2021c). Although the 2022–2023 OEWG did not produce a consensus substantive report, its discussions clarified national positions and exposed both the potential and the political limitations of a behaviour-based approach.

Resolution 78/20 established a follow-on OEWG on reducing space threats, while resolution 78/238 envisaged a parallel OEWG on further practical measures for the prevention of an arms race in outer space (UNGA, 2023a; UNGA, 2023b). In parallel, the Group of Governmental Experts established pursuant to resolution 77/250 adopted by consensus its 2024 report on further practical measures for the prevention of an arms race in outer space. The report considered substantial elements of an international legally binding instrument and recognised the possible complementary contribution of transparency and confidence-building measures (UNGA, 2024a).

General Assembly decision 79/512 subsequently convened a single Open-ended Working Group on the Prevention of an Arms Race in Outer Space in All Its Aspects for the period 2024–2028, replacing the two working groups envisaged under resolutions 78/20 and 78/238 (UNGA, 2024b). Its third session was held in Geneva from 6 to 10 July 2026 and addressed threats to space systems, transparency and confidence-building measures, responsible behaviours and possible options for strengthening the international normative framework (UNODA, 2026). The current process therefore places legally binding and non-legally binding approaches within a common deliberative framework while preserving their different legal character.

A particularly concrete measure is General Assembly resolution 77/41, which calls upon States to commit not to conduct destructive direct-ascent anti-satellite missile tests (UNGA, 2022). The measure constitutes a political commitment rather than a treaty prohibition or a general moratorium on anti-satellite capabilities. Its scope is deliberately narrow: the testing of destructive direct-ascent anti-satellite missiles. That precision contributes to observability and near-term feasibility, but it also means that the commitment does not address co-orbital systems, non-destructive interference, cyber operations or the operational use of an existing capability during conflict.

The institutional landscape remains divided by mandate. COPUOS is the principal United Nations forum for the peaceful uses, safety and sustainability of outer space activities. The First Committee, the United Nations disarmament machinery and UNODA address international security and arms-control questions. Practical measures may connect these communities, but institutional coordination must not erase the distinction between them. A safety contact mechanism developed in a COPUOS context, for example, should not silently acquire the function of determining hostile intent or international legal responsibility.

CONVERGENCES AND DIVERGENCES: CYBERSPACE VS. OUTER SPACE

Both domains feature dual-use infrastructure, substantial private ownership or operation, asymmetric capabilities and difficulties in distinguishing accident from deliberate interference. In each domain, a technical anomaly can have strategic consequences if information is incomplete and communication fails. Both also depend on data integrity: compromised

telemetry, ephemerides, software updates or identity credentials may be as consequential as the loss of hardware. These similarities create a plausible role for transparency, authenticated communication and cooperative incident management.

The divergences are equally important. Orbital debris is a persistent physical externality. It can expose unrelated operators and future missions to collision risk long after the event that produced it. Some cyber effects also persist, spread and cause physical damage; it would therefore be inaccurate to describe cyber incidents generally as reversible. The relevant distinction is that debris-producing activity changes a shared physical environment in a directly measurable and potentially long-lived way, whereas cyber effects vary widely in persistence, visibility and recoverability.

Attribution differs in structure. Space-domain awareness can observe launches, break-ups and many manoeuvres, but observation does not automatically establish intent, command responsibility or legal character. Cyber attribution may integrate technical indicators, infrastructure analysis, intelligence and contextual evidence; its confidence and disclosure constraints vary. In both domains, a shared evidentiary picture is difficult, but the objects of observation are different.

Operational time also varies. A conjunction warning may require decisions within hours, while vulnerability management can unfold over days or months; an active cyber intrusion may, however, demand immediate containment. The useful lesson is not that one domain is always faster. Governance mechanisms must be matched to event type, pre-authorised decision thresholds and contact availability.

Table 1. Comparative conditions for governance transfer

Dimension	Cyberspace	Outer space	Consequence for transfer
Infrastructure	Distributed digital ecosystems; extensive private ownership; rapid software change	Integrated ground, link, space and user segments; long asset lifecycles; growing private operation	Measures must cover the full space-system lifecycle and supply chain, not only spacecraft
Observation and attribution	Abundant but fragmentary telemetry; identity and control often obscured; classified evidence may be decisive	Physical events and trajectories can often be observed; intent and command remain uncertain	Notifications should distinguish observed event, assessed cause and attributed responsibility
Externalities	Effects range from temporary disruption to persistent compromise and physical harm	Debris can persist long after the initiating event, while harmful radio-frequency interference may affect multiple third parties and cross national borders for as long as the interfering activity continues	Distinguish persistent environmental effects from continuing operational interference and place greater emphasis on prevention, consultation and third-party consequences
Actors	States, vendors, cloud and telecom providers, CSIRTs, researchers, users	Launching and licensing States, agencies, operators, manufacturers, space-data providers, insurers, users	Article VI supervision makes national regulation a central implementation route
Institutional setting	UN GGE/OEWG/Global Mechanism; regional CBMs; mature incident-response communities	COPUOS, First Committee/ disarmament forums, ITU, national regulators and technical bodies	Measures should be assigned by mandate; no single forum can govern every risk
Verification and assurance	Conformance may be difficult to observe externally; audits and evidence-sharing can help	Some behaviours are externally observable; other data are proprietary or security-sensitive	Use layered indicators, third-party technical data and minimum-necessary disclosure

The transfer test yields a central conclusion: governance architecture is more portable than substantive rules. Protected contact channels, validated terminology, notification formats and capacity-building can perform similar functions in both domains. By contrast, a prohibition framed around a cyber effect cannot simply be recoded as a space prohibition, because the underlying objects, evidence and legal consequences differ.

TRANSLATING CYBER-GOVERNANCE DESIGN PATTERNS INTO SPACE PRACTICE

Cyber CBMs encourage States to publish national strategies, organisational structures and terminology. The space analogue is targeted publication of national space policy, regulatory responsibilities, licensing expectations, safety-of-flight procedures and channels for operator coordination. This is consistent with the information-exchange logic of the LTS Guidelines and the space TCBM acquis. It can reduce ambiguity about which authority receives an anomaly notification or approves a risk-reduction manoeuvre.

Transparency must be purposeful. Publishing broad doctrine without operational detail may generate little confidence, while excessive disclosure can expose command architecture or commercial information. A useful minimum package would identify competent authorities, national criteria for reportable events, public points of contact, the regulatory treatment of cybersecurity and debris mitigation, and the method for requesting consultations. A multilingual terminology annex should distinguish anomaly, interference, harmful interference, loss of command, conjunction, proximity operation, fragmentation and suspected hostile act. These terms describe different facts and should not predetermine attribution.

LTS Guideline B.1 already encourages States and international intergovernmental organisations to provide updated contact information for entities responsible for spacecraft operations and conjunction assessment. Cyber practice suggests how to make such contact information operational. A space network should include policy, technical and, where appropriate, diplomatic contacts; defined hours of availability; alternate contacts; authentication procedures; periodic validation; and escalation rules.

The network should not initially be labelled a “space security hotline”. That term could imply political authority and availability that a technical directory does not possess. A more credible first stage is a federated Space Safety and Security Points of Contact Network with separate service profiles. A conjunction service might support time-critical exchange of ephemerides. An interference service could route a complaint towards technical and ITU procedures. A suspected cyber incident could connect authorised national teams and operators under a confidentiality protocol. Strategic consultations would remain a State function.

Regular exercises are indispensable. An annual validation message and a biennial table-top exercise can reveal obsolete contacts, time-zone gaps, language problems and uncertainty about authority. Performance indicators should include successful contact validation, median acknowledgement time and the proportion of participating States with both policy and technical contacts.

Cyber incident-response practice provides a model for organising information under pressure. A Space Incident Response Playbook should define stages—detection, triage, stabilisation, evidence preservation, notification, coordinated analysis, recovery and post-incident learning—

without assuming the cause of an anomaly. It should cover the entire system: ground stations, cloud-hosted mission services, software supply chains, space and user segments, links and identity infrastructure.

Information should be separated into tiers. A basic alert could state affected service, time window, observable impact and a safe contact route. A restricted technical tier could include indicators of compromise, affected equipment, relevant orbital or radio-frequency data and mitigation status. Highly sensitive evidence would remain within authorised national or contractual channels. The schema should label confidence and distinguish fact from assessment. This design addresses two competing risks: too little information to coordinate and too much disclosure to protect security, privacy and commercial interests.

The playbook should also state what notification does not mean. Reporting an event should not constitute an admission of liability, an attribution of responsibility or consent to public disclosure. Safe-harbour arrangements, where compatible with national law, can improve early reporting. After-action reviews should produce anonymised lessons and update the playbook, mirroring mature incident-response practice.

The language of cyber due diligence is attractive because it connects knowledge, capacity and reasonable preventive action. In space governance, however, implementation should be attached to specific authorities. Article VI authorisation and continuing supervision support national licence conditions. Article IX due regard and consultations support risk assessment and communication where activities may cause potentially harmful interference. ITU rules govern harmful radio interference. Contract, procurement and insurance can supplement regulation.

Licensing requirements should be risk-based and proportionate to mission characteristics. Relevant conditions may include secure-by-design engineering, authenticated telemetry, tracking and command, separation of safety-critical functions, vulnerability management, software-update integrity, supply-chain assurance, incident response, recovery procedures, conjunction coordination and disposal reliability. A small university CubeSat should not face the identical evidentiary burden as a large constellation or a mission capable of rendezvous and proximity operations. Proportionality can be achieved through baseline controls plus additional requirements linked to operational risk.

Observable assurance need not disclose exploitable detail. Regulators can require an independent cybersecurity assessment, evidence that incident plans have been exercised, confirmation of contact validation and aggregate disposal-performance data. Operators can publish conformance statements referencing ISO/TS 20517:2024, NISTIR 8401 or comparable frameworks while sensitive audit findings remain protected.

Capacity-building is the enabling design pattern. A State cannot implement contact procedures, analyse conjunction data or investigate satellite interference without skilled personnel and institutional authority. Unequal capacity also affects legitimacy: a nominally universal norm may entrench the preferences of advanced space actors if emerging actors cannot shape or implement it.

A Space Security Capacity-Building Facility should therefore connect legal, policy and technical assistance. Modules could include national space legislation; licensing and supervision; basic space-domain awareness; conjunction assessment; spectrum coordination;

satellite cybersecurity; incident exercises; and participation in UN processes. Assistance should be demand-driven, politically neutral and sensitive to local institutional design. It should build durable national capability rather than create dependence on a single provider.

Multistakeholder participation is necessary but must be structured. Operators and manufacturers possess operational knowledge; insurers influence incentives; researchers test assumptions; civil society can contribute transparency and public-interest analysis. States remain responsible for international commitments and national supervision. Clear role allocation prevents "multistakeholder" from becoming a way to obscure accountability.

Table 2. Mapping cyber design patterns into space implementation

Cyber-derived pattern	Risk-reduction function	Space application	Legal, policy or technical anchor	Safeguards and indicators
Policy and terminology transparency	Reduces ambiguity about authority, doctrine and event description	Publish competent authorities, reporting thresholds, licensing expectations and a multilingual event glossary	LTS A.1 and A.3; 2013 and 2023 space TCBMs; Outer Space Treaty Article XI	Minimum-necessary disclosure; percentage of participants with current public profiles
Validated policy and technical points of contact	Accelerates authenticated communication and escalation	Federated, service-specific contacts for conjunctions, operational anomalies, harmful interference and cyber incidents	LTS Guideline B.1; 2013 and 2023 space TCBMs; applicable national and ITU procedures	Annual validation; alternate contacts; acknowledgement-time metrics; authentication tests
Protected crisis communications	Reduces spoofing, delay and misinterpretation	Authenticated channels for restricted operator-to-operator and State-to-State exchanges	Existing national authorities; voluntary CBM arrangements	Encryption, identity assurance, audit logs, exercises and clear authority boundaries
Cooperative incident response and assistance	Preserves evidence, coordinates mitigation and supports recovery	Tiered Space Incident Response Playbook covering ground, link, space and user segments	Article VI supervision; national incident law; UN cyber cooperation experience	Confidentiality tiers; fact/assessment labels; safe-harbour options; exercise completion
Critical-infrastructure protection and harm avoidance	Moves responsibility towards capable actors and prevention	Risk-based licensing, secure command, supply-chain assurance, conjunction coordination and disposal reliability	Articles VI and IX; ITU Constitution Article 45; LTS; ISO 24113:2023; ISO/TS 20517:2024	Proportionate requirements; independent assurance; aggregated performance data
Capacity-building and multistakeholder implementation	Reduces implementation gaps and makes participation meaningful	Integrated legal, technical and policy support for emerging space actors	LTS Section C; 2023 UNDC recommendations; national and regional cooperation	Demand-driven assistance; local ownership; trained personnel; exercise and retention metrics

CASE STUDIES

Destructive direct-ascent anti-satellite missile testing

The political commitment not to conduct destructive direct-ascent anti-satellite missile tests is the clearest contemporary example of a behaviour-specific space measure. It focuses on an activity whose immediate physical consequences—launch, intercept and debris creation—are relatively observable through national and commercial space-domain-awareness capabilities. The commitment addresses a shared externality: fragments can threaten the satellites of States and operators that were not involved in the test.

Against the transfer test, the measure performs strongly as an outer space analogue to narrowly framed cyber-restraint norms rather than as a direct transfer from cyberspace. It identifies conduct that increases systemic risk and asks States to abstain even in the absence of a new treaty obligation. The commitment is compatible with existing space law and reinforces the safety and sustainability objectives of the wider space governance framework. Its implementation is more externally observable than that of many cyber norms, while a national pledge requires comparatively limited institutional machinery. The measure is also intelligible to non-specialists, which supports transparency and reputational accountability.

Its limits are equally instructive. The commitment does not ban possession, development or operational use of every counterspace capability. It does not cover non-destructive direct-ascent tests, co-orbital systems, electronic interference, cyber operations or potentially dangerous proximity operations. A State may comply formally while pursuing other destabilising activities. The measure should therefore be treated as a focused risk-reduction commitment, not as evidence that the counterspace problem has been solved.

The broader governance lesson resembles successful cyber-norm design: specificity can precede comprehensiveness. A narrow and observable commitment may reduce immediate harm, establish a record of practice and create a platform for further discussion. Subsequent work could develop voluntary pre-launch notifications, debris-consequence assessment and post-event information exchange, while preserving legitimate security interests. Such additions would connect the political pledge to established space TCBMs rather than create a parallel framework.

The 2022 KA-SAT cyberattack

On 24 February 2022, a cyberattack disrupted Viasat's KA-SAT network shortly before Russia's full-scale invasion of Ukraine. Viasat reported that several thousand customers in Ukraine and tens of thousands of fixed-broadband customers elsewhere in Europe were affected; the European Union attributed the operation to the Russian Federation and emphasised its spillover effects (Viasat, 2022; Council of the European Union, 2022). The incident demonstrates that a space service can be strategically degraded through terrestrial network-management infrastructure without physically attacking a satellite.

The case reveals why space-system governance must cover the end-to-end architecture. A policy limited to spacecraft protection would miss compromised credentials, remote-management mechanisms, customer equipment and network segmentation. The incident also illustrates cascading effects across borders and sectors. Service degradation was not confined to a belligerent's military system; civilian users in multiple European States experienced consequences.

Cyber incident-response design patterns are therefore highly relevant. Validated technical contacts could accelerate warning to affected national authorities and downstream critical-infrastructure operators. A tiered reporting schema could share safe indicators and service-impact information without exposing the operator's full architecture. Evidence preservation and common time references would assist coordinated analysis. Recovery plans should include replacement logistics for compromised user equipment, alternative connectivity and pre-negotiated support between operators.

The case nevertheless demonstrates the limits of a simplistic cross-domain transfer. Public attribution depended on governmental assessments that combined technical, intelligence and contextual information rather than on operator telemetry alone. A shared incident-response playbook cannot determine international legal responsibility or resolve the strategic context in which an operation occurs. The attribution of malicious cyber activity affecting space systems also raises complex questions concerning evidence, State responsibility and the interaction between general international law and international space law (Li, 2024). A cooperative mechanism can improve fact-finding, coordination and resilience, but decisions concerning public attribution and response remain with competent States. Its appropriate objective is to narrow preventable uncertainty, not to depoliticise a deliberate hostile operation.

The case also supports using national authorisation and continuing supervision under Article VI as a domestic implementation route for space-system cybersecurity requirements. Article VI does not itself prescribe specific cyber controls. National licensing and procurement instruments can nevertheless require proportionate risk management, secure administration, identity and access controls, network segmentation, software-update integrity, incident exercises and recovery capability. Such requirements should be outcome-based and should refer to recognised policy and technical frameworks rather than freezing rapidly changing technical controls in primary legislation (United States, 2020; CISA, 2022; Lightman et al., 2022).

Conjunction assessment as an operational confidence-building practice

Conjunction assessment is a different kind of case: a mature safety practice that already performs several functions associated with CBMs. Operators and service providers exchange or compare orbital data, assess collision probability, contact counterparts and coordinate possible manoeuvres. NASA's Spacecraft Conjunction Assessment and Collision Avoidance Best Practices Handbook provides detailed operational guidance, while LTS Guidelines B.1–B.5 support contact information, orbital-data accuracy, assessment and coordination (NASA, 2023; UNOOSA, 2021).

The practice scores highly on functional equivalence. Its aim is to replace uncertainty with timely technical coordination. It is grounded in established safety and sustainability instruments, produces measurable indicators and can be supported by operators, national authorities and data providers. Unlike a generic declaration of peaceful intent, successful conjunction coordination leaves operational evidence: a message was acknowledged, data were exchanged, roles were clarified and an agreed or deconflicted course of action followed.

The limits concern data quality, incentives and authority. Different providers may produce different risk estimates. Operators may be reluctant to share precise ephemerides or manoeuvre plans. An active spacecraft may have no reachable owner, and both operators may initially expect the other to manoeuvre. Autonomous manoeuvring and large constellations add scale and machine-to-machine coordination challenges. A point-of-contact network must therefore be connected to common data standards, confidence descriptors and operator decision rules.

This case offers the strongest evidence for the article's main proposition: confidence is generated by repeatable, technically credible interaction. A global network need not begin with sensitive military-security notifications. It can build interoperability through safety events, validate communications and gradually establish procedures for more contested anomalies.

Safeguards must prevent safety channels from being used as covert intelligence-collection demands, and participation should not require disclosure beyond what is necessary to reduce collision risk.

LEGAL AND INSTITUTIONAL IMPLICATIONS

Complementarity, not legal substitution

Behaviour-based measures should reinforce, not replace, applicable international law. The Outer Space Treaty remains the organising legal framework. Voluntary notifications can facilitate Article IX consultations but cannot narrow the treaty's scope. Cybersecurity requirements in a national licence can help a State exercise Article VI supervision, but conformance with a technical standard does not automatically establish compliance with all international obligations. ITU procedures remain relevant to harmful radio interference even where the operational symptom is first reported through a wider space incident channel.

This layered model distinguishes four forms of authority. Treaty rules create legal obligations for States Parties. General Assembly resolutions and political commitments may articulate expectations but do not, by themselves, create treaty obligations. COPUOS guidelines and expert recommendations provide non-binding policy guidance. Technical standards specify repeatable requirements or practices and may become contractually or regulatorily binding when incorporated into national instruments. Academic analysis must preserve these distinctions to avoid overstating consensus.

The same caution applies to expert manuals. The Tallinn Manual 2.0 and the Woomera Manual are non-binding expert restatements that can clarify legal questions, organise primary sources and identify areas of agreement and disagreement. Their persuasive value derives from the quality of their reasoning and their treatment of treaties, State practice and official legal positions. They do not, by themselves, establish State consent, State practice or opinio juris, and they should not be presented as independent sources of international legal obligations.

Institutional allocation

No single institution should administer the entire proposed framework. COPUOS is well placed to facilitate safety, sustainability, capacity-building and contact information linked to the LTS Guidelines. The ITU has specialised authority and procedures concerning the international use of radio-frequency spectrum and satellite orbits. National regulators authorise and supervise non-governmental space activities. Operators and technical bodies implement engineering and incident procedures. Security commitments and arms-control questions belong in the First Committee and relevant disarmament forums.

Coordination is nevertheless required. A practical architecture should employ a common routing protocol implemented through federated, service-specific entry points rather than through a single institutional gateway. This would reduce duplication without creating a single point of operational or political failure. A conjunction alert would be routed to operator-coordination mechanisms; suspected harmful radio-frequency interference to the relevant national and ITU procedures; a cyber compromise to authorised incident-response teams and affected operators; and a request for inter-State consultation to competent diplomatic

authorities. Routing rules, authentication requirements and authority boundaries should be published, periodically tested and designed so that the initial classification of an event does not predetermine its legal character or attribution.

The architecture should also preserve inclusivity. A measure negotiated among a technologically advanced subset may be useful as a pilot, but global legitimacy requires accessible participation and capacity-building. Data providers and private operators should contribute expertise without acquiring de facto authority to define responsible State behaviour. Conversely, States should avoid technical prescriptions that cannot be implemented safely by operators.

The feasibility of this architecture will nevertheless depend on political willingness to cooperate under conditions of strategic competition. Major space powers may be reluctant to participate in mechanisms perceived as exposing operational capabilities, constraining freedom of action or creating asymmetric transparency obligations. Participation may therefore remain uneven, particularly where an event has both safety and national-security implications. At the same time, commercial actors increasingly control infrastructure, operational data and coordination capabilities at a scale capable of shaping de facto governance practice. Large constellation operators such as SpaceX and Amazon Leo (formerly Project Kuiper) illustrate why inter-State channels alone are insufficient: conjunction coordination, ephemeris exchange, cyber-incident response and increasingly automated manoeuvre decisions may depend upon privately operated systems and proprietary data. The governance challenge is therefore to integrate commercial capabilities without allowing market position or technical control to become normative authority. This reinforces the need for federated arrangements, interoperable standards, minimum-necessary disclosure and continuing public oversight (SpaceX, 2024; Amazon, 2025).

8.3 From voluntary practice to stronger commitments

Voluntary measures can serve as laboratories for future law, but progression is not automatic. A measure should be considered for formalisation only after its purpose, scope, costs and performance have been assessed. Evidence may support incorporation into national licensing, procurement rules, regional CBMs, COPUOS guidance or, in appropriate cases, a legally binding instrument. Different elements may follow different pathways.

Three conditions favour consolidation. First, the conduct must be sufficiently precise that implementation and non-implementation can be discussed fairly. Second, participation must be broad enough to avoid exporting risks to non-participants. Third, the measure must remain effective as technology and commercial practice change. Regular review clauses and outcome-based requirements can prevent premature rigidity.

IMPLEMENTATION ROADMAP

Translating the preceding analysis into practice requires a sequenced approach that reflects institutional maturity, implementation capacity and demonstrable risk-reduction value. Figure 1 summarises the proposed roadmap as a progression from the establishment of a minimum operating layer, through the operationalisation of cooperation, to the evaluation

and consolidation of measures that have proved effective. These phases are cumulative rather than self-contained, and progress should be assessed against observable operational outcomes rather than the number of policies or instruments adopted.

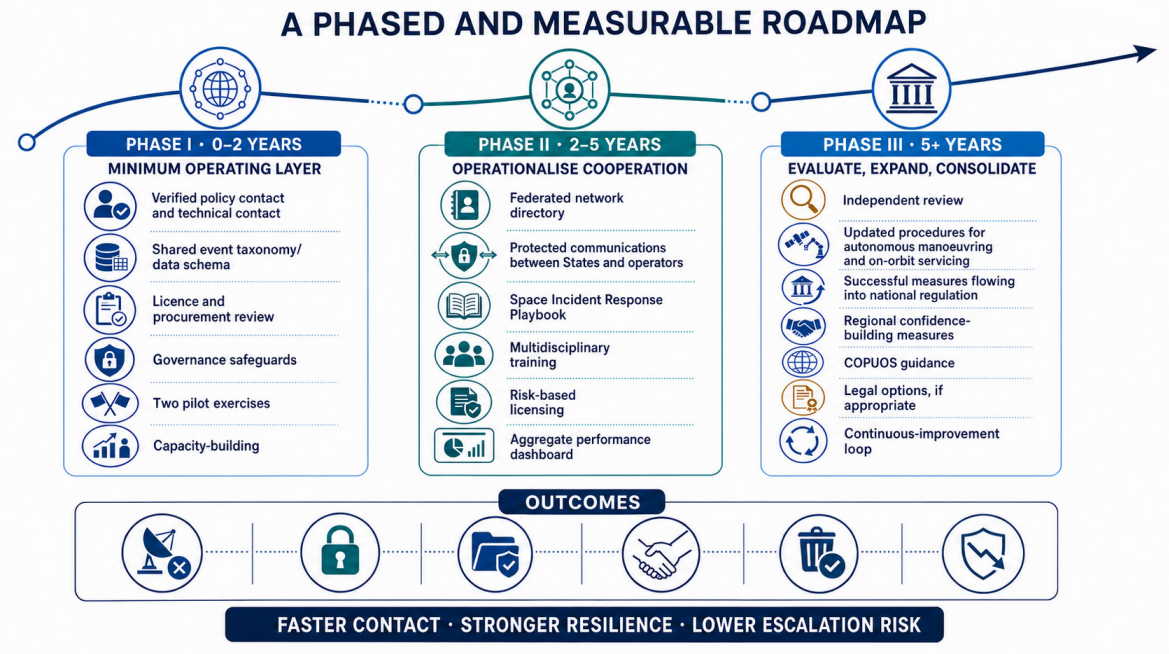


Figure 1. A phased and measurable roadmap for outer-space safety and security cooperation.

Phase I: establish the minimum operating layer (0–2 years)

Phase I should operationalise the design patterns identified in Section 6 rather than create parallel mechanisms. States should nominate and validate policy and technical contacts using existing LTS contact practices, while a small expert group comprising States, operators, incident-response teams, the ITU and relevant technical organisations should develop a common event taxonomy and minimum notification schema. National authorities should simultaneously review whether licensing and procurement frameworks adequately address end-to-end cybersecurity, conjunction coordination and post-mission disposal.

The initial governance layer should establish confidentiality tiers, authentication and data-retention requirements, clarify that notification does not constitute attribution or an admission of liability, and identify routes to formal diplomatic consultation. Pilot exercises should test at least one conjunction scenario and one cyber-enabled service disruption, with capacity-building gaps recorded as implementation requirements.

Suggested indicators are: the number and regional distribution of participating States; the proportion with both policy and technical contacts; successful annual validation rates; median acknowledgement time during exercises; the number of national frameworks reviewed; and documented capacity-building requests.

Phase II: operationalise cooperation (2–5 years)

Phase II should convert the baseline arrangements established in Phase I into routine operational practice. Participants should deploy the federated directory and protected communication arrangements, adopt and exercise the Space Incident Response Playbook,

and introduce proportionate supervisory or licensing measures for cybersecurity, incident reporting, conjunction coordination and disposal planning. Mixed exercises involving regulators, operators, cybersecurity specialists, diplomats and space-domain-awareness experts should test interoperability across institutional and national boundaries.

Procurement and contractual frameworks should allocate notification, cooperation and evidence-preservation responsibilities across operators, suppliers and service providers. Aggregate performance dashboards should provide evidence of implementation—including contact availability, exercise completion, incident-response maturity and disposal outcomes—without requiring disclosure of sensitive system information.

Indicators should include exercise frequency and participation; average time to route an event to a competent authority; the percentage of licensed high-risk missions with exercised incident plans; the rate of successful contact during conjunction events; assistance delivered against requests; and the closure rate for after-action recommendations.

Phase III: evaluate, expand and consolidate (5 years and beyond)

After a sustained period of operation, an independent review should assess whether the measures have reduced delay, uncertainty and preventable harm, while identifying under-represented regions, cost barriers, misuse risks and technological developments requiring revised governance procedures. Particular attention should be given to AI-supported and increasingly autonomous collision-avoidance and Space Traffic Management functions, autonomous spacecraft and on-orbit servicing, large-scale machine-to-machine coordination, and quantum-secure satellite communications. These technologies alter not only the technical risk environment but also the conditions under which responsibility, transparency and coordination are exercised. Increasingly automated decision-making may compress response times and complicate human oversight and accountability for manoeuvres, while AI-enabled coordination systems raise questions concerning validation, interoperability, explainability and fail-safe intervention. Quantum-secure satellite communications, in turn, introduce new dependencies across space, ground and key-management infrastructures. Governance arrangements should therefore be reviewed periodically to ensure that notification, authentication, evidence-preservation and supervision mechanisms remain effective as operational decisions become increasingly machine-mediated (ESA, 2025a; ESA, 2025b). Elements with demonstrated value may be incorporated into updated national regulations, procurement baselines, regional CBMs or future COPUOS implementation guidance. Security-specific commitments should be considered in competent disarmament forums. Where States pursue a legally binding instrument, operational evidence from voluntary implementation can improve definitions, verification design and feasibility. Measures that produce little benefit or disproportionate disclosure risk should be revised or discontinued.

Success should not be measured by the number of documents adopted. The relevant outcomes are fewer failed contacts, faster and authenticated communication, better evidence preservation, improved access to assistance, higher disposal reliability, stronger cyber resilience and fewer events in which preventable ambiguity increases escalation risk.

LIMITATIONS AND FUTURE RESEARCH

The framework requires empirical testing. Future research should compare regional implementation models, quantify contact-network performance and examine how confidentiality protections affect operator reporting. Legal analysis should explore how national space legislation can incorporate cyber risk without creating inconsistent burdens or extraterritorial conflict. Technical work is needed on interoperable event schemas, machine-readable confidence labels and the security of conjunction-data exchange.

Further case studies should address harmful radio-frequency interference, rendezvous and proximity operations, loss of positive control, software-supply-chain compromise and autonomous collision avoidance. Each raises a different combination of observability, intent and institutional competence. Research should also include insurers and finance providers, whose requirements can affect behaviour before launch, and emerging space nations, whose experience is essential to designing capacity-building that is legitimate and sustainable.

Finally, the relationship between safety and security requires continued conceptual discipline. A safety mechanism can create strategic reassurance, but it can also become politicised. A security measure may protect services while requiring sensitive disclosure. The transfer test developed here should therefore be applied event by event, with explicit legal anchors and stated assumptions.

CONCLUSION

Cyber diplomacy has demonstrated that voluntary, widely implemented behaviours—supported by transparency, points of contact, incident cooperation and capacity-building—can reduce particular risks even during geopolitical strain. Its most valuable contribution to outer-space governance is methodological. It shows how broad expectations can be decomposed into actors, procedures, safeguards and evidence of implementation.

Outer space cannot simply borrow the cyber rulebook. Debris creates persistent physical externalities; Article VI gives States a distinctive responsibility for national activities; COPUOS, the ITU and disarmament forums have different mandates; and space-domain awareness changes what can be observed without resolving questions of intent. These differences determine the substance of responsible conduct.

The practical path is therefore to borrow the method, not the code. States and industry can adapt policy transparency, validated contacts, protected communications, tiered incident reporting, cooperative assistance and capacity-building to the space environment. These measures should be anchored in the Outer Space Treaty, the LTS Guidelines, the space TCBM acquis, applicable ITU rules and proportionate national supervision. Their performance should be tested through exercises and measured against operational outcomes.

Behaviour-based governance is not a substitute for binding law. It is a risk-reduction bridge and an implementation discipline. When narrowly defined, legally compatible and institutionally legitimate, voluntary practice can lower collision, service-disruption and miscalculation risks today while generating the evidence and working relationships required for stronger arrangements tomorrow.

REFERENCE LIST

Beard, J. and Stephens, D. (eds) (2024) The Woomera Manual on the International Law of Military Space Operations. Oxford: Oxford University Press. https://doi.org/10.1093/law/9780192870667.001.0001

Committee on the Peaceful Uses of Outer Space (COPUOS) (2019) Report of the Committee on the Peaceful Uses of Outer Space, A/74/20, Annex II: Guidelines for the Long-term Sustainability of Outer Space Activities. New York: United Nations. https://undocs.org/A/74/20

Council of the European Union (2022) 'Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union', 10 May. https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

Dolowitz, D.P. and Marsh, D. (2000) 'Learning from Abroad: The Role of Policy Transfer in Contemporary Policy-Making', Governance, 13(1), pp. 5–24. https://doi.org/10.1111/0952-1895.00121

European Space Agency (ESA) (2023) Zero Debris Charter: Towards a Safe and Sustainable Space Environment. Darmstadt: ESA. https://esoc.esa.int/sites/default/files/Zero_Debris_Charter_EN.pdf

Finnemore, M. and Hollis, D.B. (2016) 'Constructing Norms for Global Cybersecurity', American Journal of International Law, 110(3), pp. 425–479. https://doi.org/10.1017/S0002930000016894

Geneva Dialogue (2025) Geneva Manual on Responsible Behaviour in Cyberspace: Chapter 2—Critical Infrastructure Protection. Geneva: DiploFoundation. https://genevadialogue.ch/wp-content/uploads/Geneva-Manual-March-2025_A4_web.pdf

International Law Commission (ILC) (2018) 'Draft Conclusions on Identification of Customary International Law, with Commentaries', Yearbook of the International Law Commission, 2018, vol. II, Part Two, A/73/10, pp. 119–156. https://legal.un.org/ilc/texts/instruments/english/commentaries/1_13_2018.pdf

International Organization for Standardization (ISO) (2023) ISO 24113:2023 Space systems—Space debris mitigation requirements. Geneva: ISO. https://www.iso.org/standard/83494.html

International Organization for Standardization (ISO) (2024) ISO/TS 20517:2024 Space systems—Cybersecurity management requirements and recommendations. Geneva: ISO. https://www.iso.org/standard/86305.html

International Telecommunication Union (ITU) (2023) Constitution of the International Telecommunication Union. Geneva: ITU. https://www.itu.int/en/council/Documents/basic-texts/Constitution-E.pdf

International Telecommunication Union (ITU) (2024) Radio Regulations, 2024 edition, Volume 1: Articles. Geneva: ITU. https://search.itu.int/history/HistoryDigitalCollectionDocLibrary/1.49.48.en.101.pdf

Kazakova, A., Radunović, V. and Droz, S. (2023) The Geneva Manual on Responsible Behaviour in Cyberspace: Implementation of Norms by Relevant Non-State Stakeholders. Geneva: DiploFoundation. https://genevadialogue.ch/wp-content/uploads/Geneva-Manual.pdf

Li, D. (2024) 'Legal Challenges of Attributing Malicious Cyber Activities against Space Activities', Leiden Journal of International Law, 37(4), pp. 963–982. https://doi.org/10.1017/S092215652400030X

Lightman, S., Suloway, T., Brule, J. and Yakaboski, S. (2022) Satellite Ground Segment: Applying the Cybersecurity Framework to Satellite Command and Control, NISTIR 8401. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8401

National Aeronautics and Space Administration (NASA) (2023) Spacecraft Conjunction Assessment and Collision Avoidance Best Practices Handbook. Washington, DC: NASA. https://nodis3.gsfc.nasa.gov/OCE_docs/OCE_51.pdf

Organization for Security and Co-operation in Europe (OSCE) (2013) Permanent Council Decision No. 1106: Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, PC.DEC/1106. Vienna: OSCE. https://cdn.osce.org/sites/default/files/f/documents/b/8/109167.pdf

Organization for Security and Co-operation in Europe (OSCE) (2016) Permanent Council Decision No. 1202: OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, PC.DEC/1202. Vienna: OSCE. https://cdn.osce.org/sites/default/files/f/documents/d/a/227281.pdf

Schmitt, M.N. (ed.) (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge: Cambridge University Press. https://doi.org/10.1017/9781316822524

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, 610 UNTS 205. https://treaties.un.org/doc/publication/unts/volume%20610/volume-610-i-8843-english.pdf

United Nations Disarmament Commission (UNDC) (2023) Report of the Disarmament Commission for 2023, A/78/42, Annex: Recommendations to Promote the Practical Implementation of Transparency and Confidence-Building Measures in Outer Space Activities. New York: United Nations. https://digitallibrary.un.org/record/4013645

United Nations General Assembly (UNGA) (2013a) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98. New York: United Nations. https://digitallibrary.un.org/record/753055

United Nations General Assembly (UNGA) (2013b) Report of the Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities, A/68/189. New York: United Nations. https://digitallibrary.un.org/record/755155

United Nations General Assembly (UNGA) (2015) Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174. New York: United Nations. https://digitallibrary.un.org/record/799853

United Nations General Assembly (UNGA) (2015a) Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/70/237. New York: United Nations. https://digitallibrary.un.org/record/815989

United Nations General Assembly (UNGA) (2020) Reducing Space Threats through Norms, Rules and Principles of Responsible Behaviours, A/RES/75/36. New York: United Nations. https://digitallibrary.un.org/record/3895440

United Nations General Assembly (UNGA) (2021a) Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, A/76/135. New York: United Nations. https://digitallibrary.un.org/record/3934214

United Nations General Assembly (UNGA) (2021b) Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report, A/75/816. New York: United Nations. https://undocs.org/A/75/816

United Nations General Assembly (UNGA) (2021c) Reducing Space Threats through Norms, Rules and Principles of Responsible Behaviours, A/RES/76/231. New York: United Nations. https://digitallibrary.un.org/record/3952870

United Nations General Assembly (UNGA) (2022) Destructive Direct-Ascent Anti-Satellite Missile Testing, A/RES/77/41. New York: United Nations. https://digitallibrary.un.org/record/3997622

United Nations General Assembly (UNGA) (2023) Reducing Space Threats through Norms, Rules and Principles of Responsible Behaviours, A/RES/78/20. New York: United Nations. https://digitallibrary.un.org/record/4030053

United Nations General Assembly (UNGA) (2023b) Further Practical Measures for the Prevention of an Arms Race in Outer Space, A/RES/78/238. New York: United Nations. https://docs.un.org/en/A/RES/78/238

United Nations General Assembly (UNGA) (2024a) Report of the Group of Governmental Experts on Further Practical Measures for the Prevention of an Arms Race in Outer Space, A/79/364. New York: United Nations. https://docs.un.org/en/A/79/364

United Nations General Assembly (UNGA) (2024b) Open-ended Working Group on the Prevention of an Arms Race in Outer Space in All Its Aspects, A/DEC/79/512. New York: United Nations. https://docs.un.org/en/A/DEC/79/512

United Nations General Assembly (UNGA) (2025) Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025: Final Report, A/80/257. New York: United Nations. https://docs.un.org/en/A/80/257

United Nations General Assembly (UNGA) (2025a) Open-ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025 Established pursuant to General Assembly Resolution 75/240, A/RES/80/16. New York: United Nations. https://digitallibrary.un.org/record/4090907

United Nations Office for Disarmament Affairs (UNODA) (2026) Open-ended Working Group on the Prevention of an Arms Race in Outer Space in All Its Aspects: Third Session, 6–10 July 2026. Geneva:

United Nations. https://indico.un.org/event/1019458/
United Nations Office for Outer Space Affairs (UNOOSA) (2021) Guidelines for the Long-term Sustainability of Outer Space Activities of the Committee on the Peaceful Uses of Outer Space, ST/SPACE/79. Vienna: United Nations. https://www.unoosa.org/documents/pdf/PromotingSpaceSustainability/Publication_Final_English_June2021.pdf
United States (2020) Space Policy Directive-5—Cybersecurity Principles for Space Systems, 4 September. Washington, DC: The White House. https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/
United States Cybersecurity and Infrastructure Security Agency (CISA) (2022) Strengthening Cybersecurity of SATCOM Network Providers and Customers, AA22-076A. Washington, DC: CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-076a
United States Government (2019) Orbital Debris Mitigation Standard Practices: November 2019 Update. Washington, DC. https://orbitaldebris.jsc.nasa.gov/library/usg_orbital_debris_mitigation_standard_practices_november_2019.pdf
Viasat (2022) 'KA-SAT network cyber attack overview', 30 March. https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/
West, J. and Azcárate Ortega, A. (2022) Norms for Outer Space: A Small Step or a Giant Leap for Policymaking?, Space Dossier 7. Geneva: United Nations Institute for Disarmament Research. https://doi.org/10.37559/WMD/22/Space/01



Ulpia-Elena BOTEZATU is a space policy, governance and security expert, former Chair of the Scientific and Technical Subcommittee of the United Nations Committee on the Peaceful Uses of Outer Space (COPUOS) for the 2024–2026 term, and currently Co-Chair of the COPUOS Action Team on Lunar Activities Consultation (ATLAC). She serves as a researcher at the National Institute for Research and Development in Informatics – ICI Bucharest and as Space Policy Officer at the Romanian Space Agency (ROSA).

Her work lies at the intersection of space governance, security, cybersecurity, critical infrastructure resilience and international space law, with a particular focus on space situational awareness, space traffic coordination, and the governance of lunar and cislunar activities. Throughout her work within COPUOS, Dr. Botezatu has contributed to international efforts addressing the safety, security and long-term sustainability of space activities, including the development of mechanisms for consultation and coordination as human and robotic activities on the Moon expand.

Dr. Botezatu's research increasingly focuses on the convergence of space security, cyber resilience, international law and emerging models of lunar governance. She holds a Ph.D. in Engineering Sciences, as well as degrees in European and International Law, complementing her technical and policy background with a legal perspective on responsibility, security, sustainability and international cooperation in outer space..



This is an open access article distributed under the terms and conditions of the
Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.