# Cyber–Space Governance: Securing Orbit through Resilient Global Traffic Management

**Philippe Goffin[1] and Gazmend Huskaj[2, 3]**
[1]Military Advisor, Permanent Representation of Belgium to the United Nations, New York, USA
[2]Geneva Centre for Security Policy (GCSP), Geneva, Switzerland
[3]Department of Computer and Systems Sciences, Stockholm University, Sweden

philippe.goffin@mil.be
g.huskaj@gcsp.ch

**Abstract:** This paper analyses the effectiveness of the international legal framework in mitigating the combined risks of orbital collision and cyber interference, and assesses how a global Space Traffic Management (STM) regime could enhance stability and security in outer space. Using Yin's single-case study design, the global space governance regime is examined through Bowen's qualitative document analysis of treaties, policies, and twelve scholarly studies, interpreted via Dunn's public-policy analysis framework. The findings show that existing instruments establish broad norms of responsibility and liability but lack operational authority, cyber-resilient procedures, and enforceable "rules of the road." Fragmented institutions and divergent national strategies perpetuate legal ambiguity and impede coordinated manoeuvre decisions. Cyber dependencies in orbital systems further magnify risks of misinterpretation and escalation. The study argues that an integrated STM regime—combining binding collision-avoidance authority, mandatory cyber-security standards, and interoperable data architectures—would materially reduce uncertainty and strengthen collective security. Policy recommendations include establishing a supranational coordination centre, codifying minimum separation and priority rules, and linking participation to verifiable cyber compliance. The proposed framework operationalises due regard through authority, assurance, and accountability, transforming space governance from permissive norms to enforceable safety mechanisms. By fusing legal, institutional, and technological dimensions, the research provides a practical pathway toward a secure and predictable orbital environment.

**Keywords:** Space governance, Cyber resilience, Cyber warfare, Space Traffic Management, Artificial intelligence, International law

## 1. Introduction

Space underpins contemporary national security, economic activity, and societal functioning by enabling communications, navigation, remote sensing, and intelligence across civil and military domains. The rapid expansion of orbital activity has, however, transformed once-predictable operating conditions into a congested and increasingly fragile environment. By 2024, space-surveillance networks tracked more than 10,000 operational satellites and over 36,000 catalogued objects, while commercial constellations such as Starlink executed tens of thousands of collision-avoidance manoeuvres annually to maintain safe separation (ESA, 2024; SpaceX, 2023). This accelerated growth—combined with uneven data sharing and the absence of unified coordination—creates conditions in which a technical malfunction, missed notification, or lost control link may be misinterpreted as intentional interference, thereby elevating escalation risks in an already volatile geopolitical landscape (Johnson, 2009).

Although early legal instruments, including the Outer Space Treaty (United Nations, 1967) and the Liability Convention (United Nations, 1972), establish principles of responsibility, liability, and due regard, they were drafted for an era of limited actors and stable trajectories. They do not reflect today's orbital environment, which is characterised by large commercial constellations, rapid manoeuvre cycles, and software-defined satellite architectures. Modern space systems rely on digitally interconnected command links, cloud-integrated ground segments, and update-driven control software. These dependencies expose orbital operations to cyber intrusions that can degrade satellite functionality, distort telemetry, or delay manoeuvres—producing physical and strategic consequences that reverberate across domains (Hallaq, 2017; Birk & Kovács, 2019; Hsu & Falco, 2023; Lykou et al., 2023). The combined effect is a dual risk: collision hazards arising from congestion and cyber-enabled disruptions that can obstruct manoeuvre execution or lead to misinterpretation of intent.

Against this backdrop, the core problem examined in this paper is twofold. First, the current international legal framework provides broad normative guidance but lacks binding, time-sensitive mechanisms for coordinated collision avoidance and digital incident response. Second, the absence of a cyber-resilient governance structure increases the likelihood that routine orbital events—whether technical faults, cyber interference, or sensor anomalies—could cascade into diplomatic disputes or security crises. This study therefore assesses the adequacy of existing legal and institutional arrangements in mitigating these risks and evaluates how a global

Space Traffic Management (STM) regime could integrate authoritative coordination, cyber-resilience, and interoperable data architectures.

The research question guiding the analysis is: *To what extent does the existing international legal framework mitigate the dual risks of orbital collision and cyber interference, and how might a global Space Traffic Management (STM) regime enhance stability and security in outer space?*

The article proceeds as follows. Section 2 reviews the scientific literature on space governance, cyber interdependencies, and emerging AI-enabled operational concepts. Section 3 outlines the methodological design. Section 4 presents empirical findings derived from qualitative document analysis. Section 5 develops the policy discussion and identifies implications for constructing an integrated and enforceable STM framework.

## 2. Reviewing the Scientific Literature

Research on space governance converges on the view that expanding satellite constellations and increasing debris densities have intensified concerns about congestion and coordination, prompting calls for more structured mechanisms to manage orbital interactions (ESA, 2024; ITU, 2022; SpaceX, 2023). Existing Space Situational Awareness (SSA) and Space Surveillance and Tracking (SST) arrangements are widely assessed as fragmented and voluntary, with scholars arguing that the absence of a global authority for manoeuvre coordination or interference attribution creates persistent operational and geopolitical vulnerabilities (EU High Representative, 2023; Stoltenberg, 2016).

Parallel scholarship extends these concerns into the cyber domain. Studies of satellite infrastructures emphasise their dependence on software-defined components, networked command links, and ground-segment connectivity, which collectively expose orbital systems to manipulation and cascading failure (Henselmann & Lehto, 2019; Birk & Kovács, 2019). Analyses of cyber operations against space assets argue that such activities can generate kinetic and strategic effects, blurring the boundary between terrestrial and orbital conflict (Hsu & Falco, 2023; Coppock et al., 2024). Research on ontology-based situational awareness models advances proposals for automated reasoning and early detection within space–cyber ecosystems, linking technical precision to operational resilience.

Artificial intelligence is increasingly positioned as a driver of this interdependence. Hallaq et al. (2017) examine machine learning as an enabler of military decision-making, noting that greater autonomy in detection and response may reduce human oversight and heighten escalation risk. Segate (2024) similarly argues that automation in space–cyberspace operations requires updated norms of attribution and accountability. Legal scholars highlight that the existing governance framework remains misaligned with these digital dynamics, lacking mechanisms for enforcement or coordinated response (Birk, 2021; Birk & Kovács, 2019; Stefoudi, 2019). Dilworth and Osborne (2022) add that although the Outer Space Treaty's responsibility and liability provisions may apply to cyber operations, attribution challenges and weak enforcement limit their practical utility during time-critical incidents. Gompert and Libicki (2023) complement these arguments by framing "detect and engage" as an emerging operational paradigm in which AI-enabled sensing, distributed space systems, and cyber operations accelerate decision cycles across domains.

Parallel Chinese research reinforces these themes from a technical perspective. Liu et al. (2023) propose ontology-based situational awareness models for space–cyber threats, complementing legal and institutional analyses of deterrence. Across this scholarship, three insights recur: (1) the legal inadequacy of existing space governance instruments to address cyber-enabled risks; (2) the deepening technical interdependence between orbital and digital infrastructures; and (3) an emerging consensus that a cyber-resilient Space Traffic Management (STM) regime is needed to integrate ontological awareness, AI-assisted defence, and enforceable coordination.

## 3. Methods and Materials

This study adopts a mono-method qualitative research design consistent with Yin's (2018) single-case study approach. The "case" under examination is defined as the global space governance regime—a bounded system comprising international treaties, national policies, and institutional frameworks governing activities in outer space. This case was selected due to its central relevance to the research problem: the inadequacy of existing legal and institutional mechanisms to manage risks arising from the intersection of space traffic, cyberspace operations, and international security. The single-case design enables an in-depth contextual analysis of this

governance structure within its real-world setting, where the boundaries between legal, technological, and strategic dimensions are interdependent.

Data collection followed the logic of triangulated documentary evidence, drawing from two primary sources. First, a structured literature review was conducted using the Scopus database to identify peer-reviewed publications addressing cyberspace operations, satellite vulnerabilities, and cybersecurity governance between 2015 and 2025. Boolean operators:

> *{satellite} AND ("cyber operation*" OR "offensive cyber*" OR "cyber warfare" OR "cyber conflict*" OR "cyber defence" OR "cyber defense") AND ("satellite*" OR "space system*" OR "orbital" OR "space asset*" OR "spacecraft") OR (( Cyber* AND "vulnerab*" ) AND ( "satellite communication*" OR "SATCOM" OR "space network*" OR "ground station*" )) OR (("space traffic management" OR "STM" OR "space governance" OR "outer space law" OR "international law") AND ("cyber secur*" OR "cyber norm*" OR "cyber governance" OR "digital resilience" OR "information assurance"))*

were applied to capture the conceptual breadth of the field. The query initially yielded 119 results; after refinement and screening based on relevance, citation frequency, and data accessibility, a final corpus of twelve academic articles was retained for detailed review. Second, primary legal and institutional documents—including United Nations treaties, European Union policies, national space directives, and official reports—were examined to provide the empirical foundation for the analysis.

Data analysis employed Qualitative Document Analysis (QDA) as formulated by Bowen (2009). This involved systematic skimming, detailed reading, and iterative interpretation of the selected materials to identify patterns, principles, and governance gaps. Analytical emphasis was placed on tracing how international law and institutional mechanisms address, or fail to address, cyber–space interdependencies. Dunn's (2018) public policy analysis framework was applied as the interpretive lens to translate these empirical findings into policy insights and recommendations. Through this integrated approach, the study aligns Yin's contextual depth with Bowen's methodological discipline and Dunn's analytical reasoning, generating a comprehensive understanding of the structural, legal, and normative dimensions of global space governance.

## 4. Results

This section presents the findings of a qualitative document analysis (QDA) of the current global space governance regime as it intersects with cyberspace operations and space traffic management. The corpus comprised foundational United Nations treaties and principles, recent UN policy texts, regional and national policy artefacts, and twelve peer-reviewed sources addressing cyberspace operations, AI-enabled defence, and space governance. The analysis identifies recurring categories that structure the empirical record: the evolution of governance instruments; emerging cyber dependencies in orbital systems; institutional fragmentation and legal ambiguity; national and regional policy divergence; and the technological integration and automation dilemma. Findings are descriptive and evidence-based, reporting what the documents contain and how patterns recur across sources.

### 4.1 The Evolution of Space Governance Instruments

Across the legal corpus, the baseline architecture for space activities is stable in its core obligations yet sparse in operational detail. The Outer Space Treaty establishes responsibility, liability, and due regard duties, with States bearing international responsibility for national activities, including those of non-governmental entities (United Nations, 1967). The Liability Convention further specifies compensation for damage caused by space objects, while the Registration Convention obliges delivery of orbital data to a central registry (United Nations, 1972a; United Nations, 1972b). In the analysed texts, these instruments provide a permissive legal envelope rather than granular navigation rules. The treaty language contains no codified priorities for "right-of-way," minimum separation standards, or binding collision avoidance procedures applicable to routine on-orbit operations outside manoeuvre and launch contexts (United Nations, 1967). The Agreement Governing Activities on the Moon contains more specific coordination references but confines them to lunar environments (United Nations, 1979).

Soft-law sources bridge some gaps but remain non-binding. The 1964 Declaration reaffirms State responsibility and enables consultations where potentially harmful interference is foreseen, yet it leaves initiative, timelines, and decision authority undefined (UN General Assembly, 1964). Subsequent principles on direct broadcasting, remote sensing, nuclear power sources, and international cooperation add sectoral process guidance and ITU-mediated frequency coordination but do not institute live orbital traffic deconfliction mechanisms (UN General

Assembly, 1983; 1987; 1993; 1997). Recent UN system texts—such as the Guidelines for the Long-Term Sustainability (LTS) of Outer Space Activities—articulate best practices for mission planning, data sharing, and risk reduction, without establishing an enforcement locus for trajectory conflict resolution (UN OOSA, 2021).

The "Pact for the Future" identifies discussion tracks for space traffic, debris, and resources, thereby signalling agenda-setting rather than an operational governance shift (UN General Assembly, 2024). Taken together, the instruments exhibit continuity in high-level norms and persistent absence of prescriptive "rules of the road," a pattern that underpins subsequent empirical categories concerning cyber-physical integration and traffic management interfaces (United Nations, 1967; 1972a; 1972b; 1979; UN OOSA, 2021; UN General Assembly, 2024).

### 4.2 Emerging Cyber Dependencies in Orbital Systems

Across the technical and policy literature, orbital infrastructures are increasingly co-constituted with cyber capabilities that enable, expose, and configure operational behaviours. Peer-reviewed studies describe satellite networks as networked information systems reliant on protocol stacks, ground segment connectivity, and cloud-mediated services, with vulnerabilities spanning denial-of-service, malicious code insertion, and data exfiltration across RF and IP layers (Aviv & Ferri, 2023; She et al., 2017; Xu, 2024). Analysis of moving-target defence (MTD) in satellite internet prototypes demonstrates that pseudo-random address and port hopping can increase attacker cost without significant throughput penalties, indicating a direction of travel toward dynamic cyber manoeuvres at the network edge of orbital architectures (Xu, 2024). Legal scholarship reveals that cyberspace operations against space systems can manifest as interference with command links, data links, or payload integrity, raising attribution and remedy questions under existing space and general international law (Schmitt & Vihul, 2017).

Empirical reporting on the Russia–Ukraine armed conflict provides concrete instances of cyber–space interdependence. Wiper operations, DDoS campaigns, and the Viasat KA-SAT incident illustrate how cyber effects can degrade space-enabled services, while commercial LEO broadband constellations supplied resilient communications and positioning-navigation-timing (PNT) workarounds through software updates and constellation-level redundancy (Aviv & Ferri, 2023). The same sources document accelerated migration of governmental data from damaged on-premises facilities to public cloud platforms and partner-hosted private clouds outside the national territory, thereby re-situating space-derived data flows within distributed digital infrastructure subject to varied legal jurisdictions (Aviv & Ferri, 2023).

At the interface of cyber and electromagnetic operations, analyses of spectrum-centred tactics describe how jamming, spoofing, and cyber payloads co-evolve, with Intelligence, Surveillance, and Reconnaissance (ISR) systems and command-and-control relying on assured spectrum access and cyber-hardened communication links (Young, 2017). Across documents, the empirical pattern is a deepening reliance on software-defined, cloud-connected, and update-driven control surfaces for orbital systems, which couples cyber resilience properties to space traffic safety outcomes via command availability, data integrity, and timing assurance (Aviv & Ferri, 2023; She et al., 2017; Xu, 2024; Young, 2017). This dependency anchors subsequent findings on the adequacy of institutional arrangements to accommodate cyber-physical risk within traffic management.

### 4.3 Institutional Fragmentation and Legal Ambiguity

The document set consistently records a dispersion of roles across technical standard-setters, national regulators, and international bodies, with limited consolidation around an entity empowered to issue binding orbital deconfliction instructions. COPUOS processes, including the LTS Guidelines, emphasise voluntary practices and information exchange, while ITU coordination focuses on frequencies and orbital slots, not operational manoeuvre authority for collision risk events (UN OOSA, 2021). Legal analyses highlight that, while the liability and responsibility framework supplies post-hoc remedies and State-to-State accountability, it does not specify pre-emption thresholds, procedural priorities, or operational control for time-sensitive conjunctions involving mixed public–private constellations (Schmitt & Vihul, 2017). Recent UN policy texts call for exploring frameworks on traffic and debris, yet they stop short of allocating decision rights or establishing supranational service provision for space traffic management (UN General Assembly, 2024).

Parallel institutional initiatives aim to fill cyber-specific gaps but remain emergent. Drafting efforts for cybersecurity standards tailored to outer space missions and critical infrastructure—surveyed in the technical governance literature—map candidate control baselines and assurance processes, often drawing from terrestrial frameworks and CCSDS security work, without an associated compliance jurisdiction in orbit (Segate, 2024). Concept papers on "assured cyber deterrence" in space document doctrinal debates around

"hacking back," malware pre-positioning, and "booby traps," illustrating how proposed cyber response logics intersect with the neutral-use and due-regard obligations of space law in the absence of authoritative interpretive guidance (Ting & Lin, 2020). The accumulated materials therefore show an institutional landscape where voluntary guidelines, sectoral standards, and national practices co-exist, but where neither treaty text nor standing body assigns operational authority for collision avoidance when cyber availability or integrity constraints affect manoeuvre timelines. This fragmentation conditions the national policy divergence recorded in the next category.

### 4.4 National and Regional Policy Divergence

Policy texts reveal differing national and regional approaches to space traffic management and cyber–space risk governance. The United States' 2018 Space Traffic Management Policy identifies flight-safety challenges and positions national leadership, industry solutions, and best-practice diffusion as primary levers, with limited appetite for delegating traffic control to multilateral entities (White House, 2018). European materials in the corpus describe multiple SSA/SST initiatives and data-sharing arrangements supported by the EU and ESA, yet note the absence of a comprehensive STM policy allocating coordination or control for avoidance manoeuvres across Member States (EU High Representative, 2023; ESA, 2024). The reviewed texts characterise China's posture through technical and standards-oriented publications and national capability development, with growing attention to active cyber defence at network and platform layers in satellite internet contexts (The State Council of the People's Republic of China, 2021; Xu, 2024; Segate, 2024). In the UN arena, the "Pact for the Future" places STM, debris, and resources on the intergovernmental agenda and invites private sector participation, but does not harmonise State preferences regarding locus of control (UN General Assembly, 2024).

Empirical accounts from the Russia–Ukraine conflict show how national strategies shape cyber-resilient operations using public–private assemblages. Ukraine's migration of sensitive registries to public clouds and to allied-hosted private infrastructure, combined with the adoption of commercial LEO broadband for continuity under kinetic and cyber stress, depict a resilience pathway grounded in diversified jurisdictional and commercial arrangements rather than a unified international traffic authority (Aviv & Ferri, 2023). Regional telecom measures, including internal roaming and inbound roaming blocks, further illustrate how national instruments condition service continuity and exposure in crisis, with secondary effects on spectrum and network management for satellite-backed services (Aviv & Ferri, 2023). The materials thus indicate variation in governance choices—lead-nation versus multilateral coordination, public cloud reliance versus on-premises control—that collectively produce a patchwork of practices relevant to traffic safety when cyber availability determines manoeuvre execution windows.

### 4.5 Technological Integration and the AI–Automation Dilemma

Across defence, security, and engineering sources, AI-enabled functions are increasingly embedded in space and cyberspace operations, raising documentable questions about control allocation, assurance, and failure modes. Reviews of AI in military cyber contexts describe learning-based detection, decision support, and autonomy for ISR, command-and-control, and defensive cyber manoeuvre, situating these capabilities within dual-use trajectories (Hallaq, 2017). Maritime cybersecurity research on dual-use AI offers parallel empirical observations on automated anomaly detection, adversarial adaptation, and model governance, which are transferable to spaceborne and ground segment networks that share protocol and operations patterns (Aldhaheri et al., 2020). Operational concepts emphasising "detect and engage" in contested electromagnetic and cyber environments report increased dependence on rapid machine-assisted sense-making and decision cycles, with electromagnetic control and cyber persistence viewed as central to force employment (Deptula & Bacon, 2019; Young, 2017).

Within the space domain specifically, security scholarship documents proposals for pre-positioned code, active countermeasures, and automated responses to cyber intrusion on spacecraft and ground segment systems, noting potential intersections with space law obligations in the absence of agreed interpretations (Ting & Lin, 2020; Schmitt & Vihul, 2017). Observational materials from the Russia–Ukraine conflict capture software-based mitigation at constellation scale, including over-the-air code changes to counter jamming and sustain PNT-related services, underscoring the operational reality of software-defined remediation in orbit (Aviv & Ferri, 2023).

The technical governance literature registers contemporaneous efforts to draft cybersecurity standards for space missions—threat models, control families, and assurance artefacts—without a clear mapping to traffic

management decisions when automated cyber responses affect attitude control, propulsion commands, or conjunction screening timelines (Segate, 2024). The pattern across documents is an integration of AI and automation into cyber-space operations that improves detection and continuity while complicating accountability chains and temporal coupling with STM processes. This linkage provides the empirical basis for evaluating adequacy of current governance in subsequent discussion. Table 1 summarises the core governance gaps identified across the legal, institutional, cyber, and technological dimensions.

**Table 1: Summary of Governance Gaps**

| Dimension | Key Gap Identified | Evidence Sources | Implication for STM |
|---|---|---|---|
| **Legal** | No "rules of the road," unclear priority rights | OST 1967, Liability Convention 1972 | No binding authority for time-critical manoeuvres |
| **Institutional** | Fragmented roles, voluntary data sharing | COPUOS LTS, ITU regulations | No central coordination for deconfliction |
| **Cyber** | Vulnerable command links, no cyber baselines | Birk & Kovács 2019; Hsu & Falco 2023 | Cyber interference can delay or distort manoeuvres |
| **Technological** | AI automation without governance | Hallaq 2017; Segate 2024 | Machine-speed decisions create accountability gaps |

## 5. Discussion

The answer to the research question, To what extent does the existing international legal framework mitigate the dual risks of orbital collision and cyber interference, and how might a global Space Traffic Management (STM) regime enhance stability and security in outer space?, is that current instruments partially shape responsible conduct yet fail to govern time-critical deconfliction or cyber-physical interdependence. The present framework constrains overtly harmful behaviour and clarifies post-hoc responsibility, but it does not allocate decision rights for live conjunction management or define cyber-resilient operating procedures. A global STM regime that fuses authoritative traffic coordination with mandatory incident reporting, interoperable data exchange, and baseline cyber hygiene would materially reduce collision likelihood, dampen misinterpretation, and enhance strategic stability. In practice, progress depends on aligning legal, institutional, and technological arrangements to support predictable manoeuvre decisions under conditions of uncertainty and time pressure.

The results reveal structural weaknesses in law, authority, and technology. Current regulations define responsibility and liability after incidents but do not specify who has priority, what distance is safe, or how manoeuvre decisions are made. Institutions promote cooperation and information exchange but lack the authority to issue binding instructions when collision risks arise. Satellites depend on software-based control, cloud connectivity, and constant updates, exposing them to cyber disruptions that delay or distort manoeuvres. The problem is systemic: rules exist without enforcement, coordination mechanisms without command authority, and safety processes that rely on unstable communication links. Without integration of these elements, routine events in orbit can be misread as deliberate acts, generating disputes over intent and responsibility.

The data also indicate growing collision risks, increased automation, and greater uncertainty about intent. Expanding constellations compress decision time and require automated systems to filter and prioritise manoeuvres. As autonomy advances, actions occur at machine speed, reducing transparency and complicating verification. Cyber operations targeting ground systems or command links can disrupt control and appear as deliberate obstruction. National approaches will continue to diverge, with some favouring market solutions and others multilateral coordination. Without a shared baseline for space-traffic management, the orbital environment will face higher near-miss rates, inconsistent manoeuvre policies, and restricted data exchange that weakens collective awareness. The main risk is not intentional attack but misjudged behaviour, where technical failure or interference is read as aggression under stress.

Policy measures should aim for steady progress that links traffic authority to cyber resilience. A coordination function should be established with the power to issue time-bounded avoidance directives under transparent procedures and review mechanisms. Clear and technology-neutral operating rules are needed, defining separation thresholds by orbital regime, priority based on mission and manoeuvre capability, and agreed timelines for response. Participation must require baseline cyber controls, including authentication of command links, integrity protection for tracking data, and timely disclosure of incidents. A federated data structure should merge public and commercial sources under verifiable quality standards and auditable access.

Incentives should align through insurance discounts for compliance, launch licensing tied to adherence, and procurement preferences for transparent data-sharing. These reforms must balance national sovereignty, commercial confidentiality, and the cost of upgrading existing systems.

Monitoring must translate these reforms into measurable indicators. Safety metrics should include collision probabilities, near-miss counts, and average delay from alert to manoeuvre. Cyber-resilience metrics should track link availability, verified data integrity, and the number of cyber incidents that impede operations. Governance metrics should measure data convergence across providers, participation rates, compliance with directives, and the timeliness of reporting. Capability metrics should record operators with verified contingency modes, independent verification coverage, and the frequency of joint exercises. Together, these indicators enable adaptive learning, targeted support, and proportionate responses when safety thresholds are crossed.

Evaluation criteria should be defined in advance to maintain focus and prevent goal drift. Effectiveness should test whether collision risk and ambiguity about intent decline over time. Efficiency should assess whether coordination costs are justified by fewer claims, outages, and debris growth. Equity should examine the effects on new entrants, ensuring fair access and manageable obligations. Legality and legitimacy must consider consistency with treaties, transparency in decision-making, and due-process safeguards. Resilience should test whether the regime withstands cyber or sensor failures without cascading disruption. Evidence should include baseline-to-outcome comparisons, post-incident analysis, and red-team testing of automated decision tools. Where performance fails to meet standards, corrective clauses should trigger procedural or technical revision. Feasibility depends on institutional design, decision rights, and sequencing.

A treaty-anchored framework should establish a coordination centre with a narrow mandate to issue avoidance directives under defined conditions. Broader participation can follow through mutual recognition of national licences embedding STM and cyber requirements. Interoperability should rely on open technical standards for data formats, encryption, and interface testing. Funding may combine assessed contributions for shared functions, user fees for premium services, and penalties for non-compliance that finance remediation. Disputes should be resolved through two tracks: fast-track technical adjudication for manoeuvre conflicts and a slower legal process for liability claims. This sequencing lowers entry barriers while maintaining a clear path toward enforceable coordination.

Risk management must address automation failures, malicious behaviour, and compromised data. Autonomy must include human-in-the-loop thresholds, verified fallback modes, and independent validation of critical decisions. Agreed “hold” protocols should define when to suspend manoeuvres during catalogue errors or cyber incidents. Data exchanges must follow zero-trust principles with continuous verification of ground and onboard systems and cryptographic provenance for trajectory data. Electromagnetic protection should complement cyber controls, as jamming and spoofing often coincide with data manipulation. Confidence-building should include direct communication channels between operators, post-incident reviews, and anonymised reporting to improve learning and accountability.

An effective traffic-management system must also accommodate commercial activity and innovation. Data-trust models can support analysis of sensitive orbital data without disclosing proprietary details. Tiered access can separate safety-critical information from competitive services. Regulatory sandboxes can test automation in controlled environments, expanding only after proven reliability. Support for emerging spacefaring nations should include tools, training, and subsidised certification to ensure equitable participation and reduce systemic risk from uneven capacity. Over time, better data, clearer rules, and trusted automation reinforce each other—improving safety and preserving accountability.

The implications for governance and international security are clear. A system that integrates authority, assurance, and accountability can turn a permissive legal framework into an operational safety regime. Coupling traffic management with secure infrastructures and measurable performance strengthens trust, narrows uncertainty, and limits escalation. This approach does not replace existing treaties or national interests; it translates due-regard obligations into shared procedures, verified data, and coordinated action. The discussion thus prepares the ground for final policy conclusions, a phased implementation roadmap, and further research on human–machine coordination, liability in automated decisions, and the governance of adaptive systems that will shape the future of orbital safety.

## Acknowledgements

Artificial intelligence tools were used only to assist with research organisation and language editing. All analysis, interpretation, and conclusions are the authors' own. Consistent with Nature's (2023) guidelines, AI tools are not credited as authors.

Ethical declaration: The study involved no human participants or sensitive data, so ethical approval was not required.

**Disclaimer:** The views expressed in this paper are solely those of the authors and do not necessarily reflect the official policies or positions of the Belgian Armed Forces, the Government of Belgium, the Geneva Centre for Security Policy, or Stockholm University. The analysis and conclusions are presented for academic and policy discussion purposes only.

## References

Aviv, I., & Ferri, U. (2023). *Russian–Ukraine armed conflict: Lessons learned on the digital ecosystem.* International Journal of Critical Infrastructure Protection, 43, 100637. https://doi.org/10.1016/j.ijcip.2023.100637

Birk, A. M. (2021). Legal and policy aspects of satellite and space traffic management. *Space Policy, 57,* 101420.

Birk, A. M., & Kovács, L. (2019). Cyber operations in satellite infrastructures: Emerging vulnerabilities and policy responses. *Journal of Cybersecurity, 5*(3), tyz013.

Bowen, G. A. (2009). *Document analysis as a qualitative research method. Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Coppock, A., Jensen, R., & Lavigne, D. (2024). Artificial intelligence in maritime cybersecurity: Dual-use applications for defence and offence in the age of digital seas. *Defence Studies, 24*(2), 198–215.

Dilworth, S. W., & Osborne, D. D. (2022). *Cyber threats against and in the space domain: Legal remedies*. In T. Jančárková, G. Visky, & I. Winther (Eds.), 2022 14th International Conference on Cyber Conflict: Keep Moving (pp. 235–247). NATO Cooperative Cyber Defence Centre of Excellence.

European Space Agency. (2024). *Space environment statistics · Space debris user portal.* https://sdup.esoc.esa.int/discosweb/statistics/

European Union High Representative for Foreign Affairs and Security Policy. (2023). *European Union space strategy for security and defence.* https://ec.europa.eu/transparency/documents-register/detail?ref=JOIN(2023)9&lang=en

Gompert, D. C., & Libicki, M. (2023). Detect and engage: A new American way of war. *Survival*, 65(5), 65–74. https://doi.org/10.1080/00396338.2023.2261246.

Hallaq, B., Somer, T., Osula, A.-M., Ngo, K., & Mitchener-Nissen, T. (2017). Artificial intelligence within the military domain and cyber warfare. *Journal of Information Warfare, 16*(4), 55–68. https://wrap.warwick.ac.uk/id/eprint/104774

Henselmann, G., & Lehto, M. (2019). Where cyber meets the electromagnetic spectrum. In T. Cruz & P. Simões (Eds.), *Proceedings of the 18th European Conference on Cyber Warfare and Security (ECCWS 2019)* (pp. 209–218). Academic Conferences International.

Hsu, J., & Falco, G. (2023). *Space booby traps: Hacking back and assured cyber deterrence in space.* In *2023 IEEE International Conference on Assured Autonomy (ICAA)* (pp. 115–118). IEEE. https://doi.org/10.1109/ICAA58325.2023.00024.

International Telecommunication Union. (2022). *E-submission of satellite network filings.* https://www.itu.int/ITU-R/space/asreceived/Publication/DisplayPublication/23706

Johnson, N. (2009). *The collision of Iridium 33 and Cosmos 2251: The shape of things to come.* NASA Technical Reports Server. https://ntrs.nasa.gov/api/citations/20100002023/downloads/20100002023.pdf

Kovács, L., & Tóth, K. (2019). Cyber threats to space systems and implications for national security. *Journal of Strategic Security, 12*(4), 75–90.

Liu, B., Yi, J., Yao, L., Wang, Y., Ding, Z., & Zhu, X. (2023). 面向太空网络战威胁的态势感知本体建模 [Ontology-based situational awareness for space cyber threats]. *Journal of Cybersecurity Science and Technology, 8*(1), 33–46.

Lykou, S., Gritzalis, D., & Theocharidou, M. (2023). Cybersecurity of space systems and satellite communication infrastructures. *Acta Astronautica, 206,* 141–156.

Nature Editorial. (2023). *Tools such as ChatGPT threaten transparent science; here are our ground rules for their use*. *Nature*, 613, 612. https://doi.org/10.1038/d41586-023-00191-1

Stefoudi, D. (2019). *The relevance and applicability of cybersecurity laws with regard to data storage on board satellites and on the ground*. Air & Space Law, 44(4–5), 425–444.

SpaceX. (2023). *SpaceX Gen 1 semi-annual report.* https://licensing.fcc.gov/myibfs/download.do?attachment_key=23204338

Stoltenberg, J. (2016). *Press conference following the meeting of the North Atlantic Council at the level of Heads of State and/or Government.* North Atlantic Treaty Organization. https://www.nato.int/cps/en/natohq/opinions_171554.htm

The State Council of the People's Republic of China. (2021). *China's space program: A 2021 perspective.* https://english.www.gov.cn/archive/whitepaper/202201/28/content_WS61f35b3dc6d09c94e48a467a.html

UN General Assembly. (2024). *Pact for the Future, Global Digital Compact and Declaration on Future Generations.* https://www.un.org/sites/un2.un.org/files/sotf-pact_for_the_future_adopted.pdf

United Nations General Assembly. (1964). *Declaration of legal principles governing the activities of states in the exploration and use of outer space (18th session).* United Nations Digital Library. https://digitallibrary.un.org/record/203965

United Nations General Assembly. (1983). *Principles governing the use by states of artificial Earth satellites for international direct television broadcasting (37th session).* United Nations Digital Library. https://digitallibrary.un.org/record/41084

United Nations General Assembly. (1987). *Principles relating to remote sensing of the Earth from outer space (41st session).* United Nations Digital Library. https://digitallibrary.un.org/record/126423

United Nations General Assembly. (1993a). *Declaration on international cooperation in the exploration and use of outer space for the benefit and in the interest of all states, taking into particular account the needs of developing countries (51st session).* United Nations Digital Library. https://digitallibrary.un.org/record/231739

United Nations General Assembly. (1993b). *Principles relevant to the use of nuclear power sources in outer space (51st session).* United Nations Digital Library. https://digitallibrary.un.org/record/159141

United Nations Office for Outer Space Affairs. (2021). *Guidelines for the long-term sustainability of outer space activities of the Committee on the Peaceful Uses of Outer Space.* https://www.unoosa.org/documents/pdf/PromotingSpaceSustainability/Publication_Final_English_June2021.pdf

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.* United Nations Treaty Series. https://treaties.un.org/doc/Publication/UNTS/Volume_610/volume-610-I-8843-English.pdf

United Nations. (1972a). *Convention on registration of objects launched into outer space.* United Nations Treaty Series, 1023(1), 15020. https://treaties.un.org/doc/Publication/UNTS/Volume_1023/volume-1023-I-15020-English.pdf

United Nations. (1972b). *Convention on the international liability for damage caused by space objects.* United Nations Treaty Series, 961(1), 13810. https://treaties.un.org/doc/Publication/UNTS/Volume_961/volume-961-I-13810-English.pdf

United Nations. (1979). *Agreement governing the activities of states on the Moon and other celestial bodies.* United Nations Treaty Series, 1363, 23002. https://treaties.un.org/doc/Publication/UNTS/Volume_1363/volume-1363-I-23002-English.pdf

Vecellio Segate, R. (2024). Drafting a cybersecurity standard for outer-space missions on critical infrastructure: China and the West. *Computers & Security, 138,* 103749. https://doi.org/10.1016/j.cose.2024.103749

White House. (2018). *Space Policy Directive-3: National Space Traffic Management Policy.* https://trumpwhitehouse.archives.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/

Xu, R. (2024). 基于移动目标防御的卫星互联网防御系统设计 [Design of satellite Internet defense system based on mobile target defense]. *Space-Integrated-Ground Information Networks, 5*(4), 107–112. https://doi.org/10.11959/j.issn.2096-8930.2024043.

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). Thousand Oaks, CA: SAGE Publications.