

Verification 2.0: A New Approach to Outer Space Security Verification

Thomas G. Roberts

October 2026

GCSP Policy Brief No.27



GCSP
Geneva Centre for
Security Policy

Geneva Centre for Security Policy

The Geneva Centre for Security Policy (GCSP) is an international foundation that aims to advance global cooperation, security and peace. The foundation is supported by the Swiss government and governed by 54 member states. The GCSP provides a unique 360° approach to learn about and solve global challenges. The foundation's mission is to educate leaders, facilitate dialogue, advise through in-house research, inspire new ideas and connect experts to develop sustainable solutions to build a more peaceful future.

The GCSP Policy Briefs Series

The GCSP Policy Briefs series addresses current security issues, deduces policy implications and proposes policy recommendations. It aims to directly inform policy- and decision-making of states, international organisations and the private sector.

Under the leadership of Ambassador Thomas Greminger, Executive Director of the GCSP, the series is edited by Professor Nayef Al-Rodhan, Director of the Geopolitics and Global Futures Department, and Doctor Tobias Vestner, Director of the Research and Policy Advice Department & Head of Security and Law, and managed by Ms Christine Garnier Simon, Administration and Coordination Manager, GCSP Geopolitics and Global Futures.

Geneva Centre for Security Policy

Maison de la paix

Chemin Eugène-Rigot 2D

P.O. Box 1295

1211 Geneva 1

Switzerland

Tel: + 41 22 730 96 00

Contact: www.gcsp.ch/contact

www.gcsp.ch

ISBN: 978-2-88947-460-8

©Geneva Centre for Security Policy, October 2026

The views, information and opinions expressed in this publication are the author's own and do not necessarily reflect those of the GCSP or the members of its Foundation Council. The GCSP is not responsible for the accuracy of the information.

About the author

Thomas González Roberts is an Assistant Professor with a joint appointment in the Sam Nunn School of International Affairs and the Daniel Guggenheim School of Aerospace Engineering at the Georgia Institute of Technology. He is the Director of Georgia Tech's [Engineering Space Policy Laboratory](#). Using tools from observational astronomy and computational astrodynamics, Roberts studies the behavior of Earth-orbiting satellites to understand how space actors – from superpowers to start-ups – engage with outer space governance. His research interests include international coordination, sustainability, and security in space. Roberts' work has been supported by the Harry S. Truman Scholarship Foundation, the National Science Foundation, and the Swiss State Secretariat for Education, Research, and Innovation, and earned recognition with the Massachusetts Institute of Technology's (MIT) Prize for Open Data, the Geneva Centre for Security Policy's Prize for Innovation in Global Security, and a placement on Forbes Magazine's 30 Under 30 in Science list. He holds a PhD and SM in aeronautics and astronautics from MIT, an SM in technology and policy from MIT, and a BA in astrophysical sciences from Princeton University.

Introduction

For decades, efforts to develop new instruments for outer space security have been plagued by the persistent recognition that adherence to new commitments would be difficult to verify.¹ That is, proposed agreements constraining particular satellite behaviours deemed mutually unacceptable by a collection of states could be easily violated without others knowing about it. While foolproof verification mechanisms are distinctly missing from some foundational instruments of space security – such as Article IV of the Outer Space Treaty (OST) that bans the placement of nuclear weapons in orbit – concerns about effective verification continue to drive contemporary discussions on the prevention of an arms race in outer space.² But the conditions that make verification challenging in space are changing. When combined, recent developments in information sharing among satellite operators and advances in space domain awareness (SDA) create new opportunities for non-intrusive verification.³ Together, their potential to support diplomacy in today's low-trust environment warrants closer study.

This Policy Brief proposes a new approach, referred to here as *Verification 2.0*, that treats verification as a structured comparison between two inputs:

1. **Declarations** by states about their satellites' planned behaviours; and
2. **Independent observations** of these satellites in operation.

By inspecting the differences between the *purported* satellite behaviour declared by states and *actual* satellite behaviour discerned by observation, any capable party can assess adherence to a certain class of space security agreements and investigate activities of concern.

This Verification 2.0 framework offers opportunities to verify not just future instruments for space security, but some existing treaties and non-binding norms that already influence behaviour in the outer space domain. The

¹ US Congress, Office of Technology Assessment (1985) *Anti-Satellite Weapons, Countermeasures, and Arms Control*, OTA-ISC-281, Washington, DC, US Government Printing Office, <https://www.princeton.edu/~ota/disk2/1985/8502/850207.PDF>.

² UN (United Nations) (1966) Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (Outer Space Treaty), art. IV, opened for signature 27 January 1967, entered into force 10 October 1967, UN General Assembly Resolution 2222 (XXI), https://www.unoosa.org/pdf/gares/ARES_21_2222E.pdf; M.P. Gleason (2024) "Charting a path through the space arms control verification challenge", Aerospace Corporation, August, <https://csp.aerospace.org/papers/charting-path-through-space-arms-control-verification-challenge>.

³ Note: In this Policy Brief, the term space *domain* awareness refers to the collection and processing of information related to space objects' physical behaviour in orbit (their orbital trajectories and how these trajectories have changed over time due to natural perturbations or their operators exerting control authority via manoeuvres) and their activity in the radio-frequency spectrum (the signals they emit and how they have changed over time). On the other hand, space *situational* awareness refers to the narrower practice of collecting information only about space objects' physical behaviour.

following section introduces the security challenges surrounding space domain awareness that inspired the framework, the third section introduces the kinds of information-sharing processes and observation practices central to it, and the fourth section demonstrates its application across three cases and considers a fourth case that tests the framework's limits.

Security Challenges

Verifying behavioural limits in outer space – such as constraints on how spacecraft should approach one another or operate while in physical proximity – is inherently challenging, because it relies on understandings of the space domain that states do not necessarily have in common. Unlike verification schemes in other domains, states characterise space activities using observational tools they do not always disclose, administered outside of any protocols enforced by an international organisation.⁴ While states enjoy security benefits from withholding the insights into satellite activities they produce or acquire, they also use these same insights to substantiate their concerns about other states' practices in the domain. When expressing these concerns in multinational forums, they reveal their willingness to disclose portions of their knowledge of space activities of interest, but only in certain contexts. The Verification 2.0 framework recognises the preference among states to withhold details about their space surveillance capabilities by providing pathways for sharing only the information needed to substantiate claims that agreed-on behavioural limits have been exceeded.

States spend upwards of billions of dollars on space surveillance missions by deploying and maintaining vast networks of ground- and space-based optical telescopes, radar systems, and radio-frequency (RF) sensors that work together to track satellites' operations as they evolve over time.⁵ Withholding details about these missions – the specifications of the sensors in their networks, the uncertainties around their measurements, and the priorities with which they observe objects of interest – is entirely rational from a security perspective. If states were perfectly transparent about what they *can* see, they would also reveal what they *cannot* see, and adversaries could use this information to evade detection. As such, it is likely not in the interests of SDA-capable states to publish data that would reveal the full extent to which they can detect and

⁴ Preparatory Commission, CBTBO (Comprehensive Nuclear-Test-Ban Treaty Organization) (2026) "Overview of the verification regime", <https://www.ctbto.org/our-work/verification-regime>; OPCW (Organisation for the Prohibition of Chemical Weapons) (2008) "The verification regime of the Chemical Weapons Convention: An overview", 28 November, <https://www.opcw.org/media-centre/news/2008/11/verification-regime-chemical-weapons-convention-overview>.

⁵ US GAO (Government Accountability Office) (2015) "Space situational awareness: Status of efforts and planned budgets", GAO-16-6R, 8 October, <https://www.gao.gov/products/gao-16-6r>; European Parliament, "Legislative Resolution of 17 April 2019 on Establishing the Space Programme of the Union", P8_TA(2019)0402, art. 11, https://www.europarl.europa.eu/doceo/document/TA-8-2019-04-17_EN.html; UK (United Kingdom) (2026) "UK Space Strategy", GOV.UK, <https://www.gov.uk/government/publications/uk-space-strategy/uk-space-strategy>.

characterise space object behaviour or the processes with which they use that information to assess threats.

At the same time, lower-resolution SDA data is readily shared by public and private entities, and has been for some time. For example, the US *Space-Track* catalogue, now maintained by the US Space Force, has spent decades describing the physical behaviour of thousands of space objects, including non-maneuvrable debris.⁶ Other states support similar efforts such as the European Space Agency's *DISCOS* catalogue or the Russian *JSC Vimpel* catalogue.⁷ In recent years, private firms have also deployed and maintained their own commercial space surveillance networks – often traversing international borders to do so – and created independent space object catalogues as one of the many data products they provide to customers.⁸ Regardless of the source, the principal feature of a space object catalogue is its collection of *orbital elements* or descriptions of orbital trajectories at particular moments in time, not raw observations from sensors or any other details that describe broader space surveillance capabilities. When orbital elements are made available for space objects around the time in which these objects are engaged in an activity of interest, they can be used to reconstruct their trajectories and estimate key parameters that describe their interactions. If these reconstructed trajectories are complemented with other selectively shared SDA data, such as RF emissions patterns, a yet richer picture of a particular episode of space activity can be established.

In recent meetings at multinational forums dedicated to space security, delegates regularly highlighted classes of space activities they considered dangerous – such as satellites being “shadowed”, approaching one another at distances as low as ten kilometres, or forcing others to perform an evasive manoeuvre – but stop short of disclosing the episodes that inspired their remarks, much less identifying or publishing any data to substantiate their claims.⁹ However, in many cases, such episodes can be reconstructed using SDA data already in the public domain or that which could be shared by willing parties, even when states do not directly do so themselves.

By identifying low-resolution SDA data in the public domain associated with particular episodes of interest or supplying it themselves if their data is not already public, states can describe the behaviours that concern them in greater detail by using operationally meaningful terms, such as the separation distance

⁶ Space-Track.org (n.d.) <https://www.space-track.org/>.

⁷ European Space Agency Space Debris Office (n.d.) DISCOSweb: Database and Information System Characterising Objects in Space, <https://discosweb.esoc.esa.int/>; T. Kruczek (2025) “JSC Vimpel”, KeepTrack, 15 April, <https://keeptrack.space/deep-dive/jsc-vimpel>.

⁸ US GAO (2023) “Space situational Awareness: DOD should evaluate how it can use commercial data”, GAO-23-105565, March, <https://www.gao.gov/products/gao-23-105565>.

⁹ EU (European Union) (2026) “Statement to the Open-ended Working Group on the Prevention of an Arms Race in Outer Space in All Its Aspects (OEWG on PAROS)”, third substantive session, Geneva, 9 July; PRC (People's Republic of China) (2026) “Statement to the OEWG on PAROS”, third substantive session, Geneva, 8 July; Netherlands (2026) “Statement to the OEWG on PAROS”, third substantive session, Geneva, 9 July.

between objects, their relative velocity, or the magnitude of the manoeuvres executed to change a satellite's orbit. In doing so, they may even make progress towards reaching common ground with one another on the very nature of behaviour limits that may prevent dangerous activities from being conducted in the future. Importantly, however, the availability of SDA data alone is not sufficient to effectively verify adherence to any agreed-on behavioural limit.

Understanding satellite behaviour in orbit requires both observation and context. Even if states more accurately understand the physics of the behaviours that concern their peers, they may not understand the contexts that underlie the latter's threat assessments. Consider a series of manoeuvres that raise an aging commercial satellite to a sparsely populated graveyard orbit. The same series of manoeuvres – the same sequence of firing thrusters, imparting the same effects – would likely be interpreted very differently if it instead were used to place a military satellite within a few kilometres of another military satellite operated by a principal adversary. Observed activities become significant only in light of context. In particular, activities in space can be classified as *anomalous* or *nominal* when compared to what spacecraft are expected to do. Some expectations of satellite activities are empirical, or inferred from observations of past behaviour. Others arise from information supplied by the states that authorise their satellites' operations, including the details they declare about their purpose, uses of the RF spectrum, or operational status.

Adherence to agreed-on behavioural limits in space can be verified when declarations of intent contextualise the activities observed in operational practice and described using SDA data.

Policy Implications

States' existing practices when declaring the intent behind their space activities and observing the behaviour of space objects can be combined to form a new approach for verifying proposed instruments of space security. The following subsections examine how these practices could work, why states might be incentivised to participate, and ways in which the framework is inherently limited.

Declaring Intent by Sharing Information

States can declare the intent behind their space activities in a variety of ways. States that ratified the Limited Test Ban Treaty, for example, effectively declared their intent to refrain from detonating a nuclear weapon in the outer space domain.¹⁰ States also declare more granular operational intent – such as their plans to use particular orbits or RF frequency bands – as part of processes

¹⁰ UN (1963) Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water (Limited Test Ban Treaty), art. I, opened for signature 5 August, entered into force 10 October, 480 UNTS 43, <https://treaties.un.org/doc/Publication/UNTS/Volume%20480/volume-480-I-6964-English.pdf>.

described in other legally binding treaties and administered on a regular basis. In some cases, commercial satellite operators publish their own descriptions of their fleets' ongoing and future activities in varying levels of detail, outside of any obligations they may have to the states that authorise their missions. Inspired by these practices, new information-sharing mechanisms for improving space *safety* proposed by states in multinational forums may also have practical effects for improving space *security* under Verification 2.0 in the future.

Today's practice of declaring intent in space is often tied with states' existing legal obligations. States parties to the Registration Convention must register their space objects with the United Nations (UN) and declare their nominal orbital neighbourhood and general purpose.¹¹ However, such declarations are both low resolution and low tempo: states can choose how much information to share in registration filings and rarely make updates as their missions evolve over time.¹² Much more descriptive and frequent declarations of intent occur as part of the administration of the International Telecommunication Union's (ITU) Radio Regulations.¹³ States that wish to protect their satellites from harmful interference in the RF spectrum must obtain network assignments from the ITU, a specialised agency of the UN, and declare the frequency bands and orbits they plan to use as part of their space missions. Because protections only apply to the frequency bands and orbits prescribed in active networks assigned to their respective states, satellite operators must limit their operations to these prescriptions in order to avoid harmful interference.¹⁴ States' filings related to their obligations to both the Registration Convention and the Radio Regulations are accessible to all other member states, but neither mechanism enforces compliance among signatories, and deviations from intent regularly occur.¹⁵

Orbital elements routinely published in space object catalogues are largely considered insufficient for reliable conjunction analysis, including collision-risk

¹¹ UN (1974) Convention on Registration of Objects Launched into Outer Space (Registration Convention), art. IV, opened for signature 14 January 1975, entered into force 15 September 1976, UN General Assembly Resolution 3235 (XXIX), https://www.unoosa.org/pdf/gares/ARES_29_3235E.pdf. Note: Registration Convention filings provide a description of a space object's nominal orbital *neighbourhood*, not its orbital *trajectory*, because descriptions of orbital trajectories require more information than the convention requires.

¹² R.S. Jakhu et al. (2018) "Critical issues related to registration of space objects and transparency of space activities", *Acta Astronautica*, 143, February, pp. 406-420, <https://doi.org/10.1016/j.actaastro.2017.11.042>.

¹³ ITU (International Telecommunication Union) (2024) *Radio Regulations*, revised by the 2023 World Radiocommunication Conference (WRC-23), entered into force 1 January 2025, <https://www.itu.int/pub/R-REG-RR>.

¹⁴ P. Shinnars and T.G. Roberts (2026) "Measuring compliance to the International Telecommunication Union's milestone approach to non-geostationary satellite frequency assignments", International Academy of Astronautics Space Traffic Management Conference, February.

¹⁵ UNOOSA (UN Office for Outer Space Affairs) (n.d.) "United Nations Register of Objects Launched into Outer Space", <https://www.unoosa.org/oosa/en/spaceobjectregister/index.html>; ITU (2026) "ITU Space Explorer", <https://www.itu.int/itu-r/space/apps/public/spaceexplorer/networks-explorer>; J.E. Ferrier and T.G. Roberts (2026) "Measuring compliance to the United Nations Registration Convention", International Academy of Astronautics Space Traffic Management Conference, February; T.G. Roberts (2024) *Measuring Compliance to the International Telecommunication Union's Geosynchronous Orbital Assignments*, PhD diss., Massachusetts Institute of Technology, Department of Aeronautics and Astronautics, May.

assessment.¹⁶ To produce more actionable collision warnings, in recent years a group of commercial actors have chosen to share their own higher-resolution descriptions of their fleets' orbital trajectories – significantly more accurate data than what can be derived from repeated observations from space surveillance sensors – outside of their legal obligations.¹⁷ A fraction of these commercial actors take a further step towards transparency, and publish their plans for how they intend to manoeuvre their satellites in the future: both via commonplace manoeuvres designed to preserve their preferred orbital characteristics and less frequent, higher-magnitude ones designed to more dramatically change their orbital trajectories. While operational constraints may prevent those operators from executing manoeuvres exactly as they had intended, manoeuvre plans offer third parties insight into operators' desired results, which they may still achieve via a similar manoeuvre at another time.

In coming years, states are poised to take lessons from these satellite operators' voluntary practices and consider non-legally binding resolutions to share similar information in the name of space safety. As part of ongoing discussions within the Expert Group on Space Situational Awareness (EG-SSA) of the Committee on the Peaceful Uses of Outer Space, states have developed draft recommendations to share information describing all of their satellites' orbital trajectories, measurements of their physical size, their abilities to perform manoeuvres, and the manoeuvres they plan to pursue.¹⁸ While these efforts are explicitly linked to preventing physical collision between satellites, they demonstrate states' willingness to share information that offers insight into one another's capabilities and near-term operational plans in orbit.

In addition to upholding their existing legal obligations or making progress on their goals in outer space safety, states may be incentivised to practise these new methods of declaring intent in order to offer greater predictability of their activities to their adversaries, which in turn lowers the likelihood of these activities being misinterpreted. Many states in the UN Open-ended Working Group (OEWG) on the Prevention of an Arms Race in Outer Space (PAROS) already advocate for measures to improve transparency and predictability, so mechanisms designed to promote declarations of intent are well situated to earn their support.

Of course, a risk associated with states declaring intent is that the information shared publicly through any of these mechanisms may not be true. In retrospect, inaccurate declarations may be explained by negligence in some cases or deceit

¹⁶ C. Levit and W. Marshall (2011) "Improved orbit predictions using two-line elements", *Advances in Space Research*, 47(7): 1107-1115, <https://doi.org/10.1016/j.asr.2010.10.017>.

¹⁷ American Institute of Aeronautics and Astronautics (2026) "Amazon Leo, Eutelsat, Iridium, and SpaceX, orbital safety best practices for satellite operators", ver. 3.0, May, <https://www.ascend.events/outcomes/satellite-orbital-safety-best-practices-guide-v3/>.

¹⁸ Expert Group on Space Situational Awareness, UN Committee on the Peaceful Uses of Outer Space (2026) "Draft Recommendations of the Expert Group on Space Situational Awareness", Recommendation 2, 12 June, https://www.unoosa.org/documents/pdf/copuos/stsc/EG%20SSA/Chairs_updated_draft_recommendations_EG_SSA_12June.pdf.

in others. Even declarations made in good faith can easily become outdated when operators' plans change, which may happen more often as military actors continue their pursuit of more dynamic space operations.

But, importantly, data shared through these mechanisms need not serve as truth. Under the Verification 2.0 framework, they serve another purpose: making states' intent explicit. Actual satellite behaviour in orbit discerned through observation can then be interpreted in the context of the purported behaviours described in states' declarations.

Independently Observing Satellite Operations

Actual satellite behaviour can be discerned using SDA analysis and compared to the purported behaviours described by states in the information they share about their operations. Under Verification 2.0, these comparisons may be made on a routine basis to identify inconsistencies of concern, or as a result of coordinated demonstrations designed for independent observers to corroborate a particular declaration.

Observing routine operations

Under a space security agreement bolstered by Verification 2.0, states may use SDA analysis to regularly monitor the space object population, detect activities that violate an agreed-on behavioural limit, and use discrepancies between the purported and actual behaviour of the satellites involved to substantiate their concerns.

For example, when observing a foreign satellite with a relatively low separation distance from one of their own, a state can characterise a satellite's observed behaviours in the context of declarations from the foreign state regarding that particular satellite. Did the foreign satellite recently perform a manoeuvre to reach its current orbital trajectory? Was this manoeuvre consistent with a declared manoeuvre plan? Is this satellite acknowledged by the state that authorised its mission as an operational and manoeuvrable spacecraft? Is it operating within the protections of an active ITU satellite network, or could its emissions harmfully interfere with those of its neighbours?

With this framing, comparing declared and observed behaviour can reveal an inconsistency that warrants further scrutiny. While such an inconsistency alone does not establish that a violation has occurred – because deviating from intent is a normal part of space mission management, and SDA data products are never free of error – it could provide further evidence for a states' concerns. When this evidence is made publicly available, third parties can evaluate the concerning activity for themselves and choose to share their own SDA data describing the episode, if available, to corroborate or contest another state's characterisations. Agreements employing Verification 2.0 could incorporate these opportunities for clarification and consultation as safeguards against premature or unfounded accusations of non-compliance.

States that do not already publish space object catalogues may be incentivised to participate in such an information-sharing exercise as a means of demonstrating their SDA capabilities and effectively informing their orbital neighbours that they are already monitoring their orbital neighbourhood. States with a more robust SDA ecosystem may choose to acquire SDA data from private companies to further describe activities of interest as a means of corroborating their publicly available catalogues and building other states' confidence in their SDA assessments.

Observing a coordinated demonstration

A space security agreement benefitting from Verification 2.0 could also provide a framework for coordinated demonstrations designed to help states build confidence in one another's declarations.

For example, a state could publish its intention to demonstrate the manoeuvrability of one of its satellites by declaring a plan for it to execute a particular manoeuvre at a particular time. Independent observers – states or firms with one or more space surveillance sensors capable of observing the satellite at the time of the purported manoeuvre – have the opportunity to observe the manoeuvre if they choose to do so.¹⁹ Others can choose to assess a publicly available space object catalogue after the fact to corroborate the declaration. In any case, third parties can benefit from the exercise by characterising the observed operation and ascertaining certain qualities of the demonstrating states' capabilities, such as the class of propulsion system most likely used as part of the manoeuvre or the change in velocity it imparted to the spacecraft.

While corroboration of this nature may build evidence for a positive claim – that is, that a state indeed possesses a certain capability – it does not establish that the observed satellite does not possess other, undeclared capabilities. While particularly SDA-capable states may be well positioned to participate, states with underdeveloped space surveillance networks may refrain from doing so, as the exercise could reveal a noticeable gap in their sensors' fields of view.

Why Apply Verification 2.0?

Verification 2.0 can contribute to a range of potential agreements intended to promote a more secure outer space domain. Some applications ask little of the states being assessed; others require them to create deliberate opportunities for observation. A final, more demanding application – the detection of a nuclear weapon onboard a satellite – represents a timely edge case.

¹⁹ Note: If the manoeuvre is low-thrust and executed over a prolonged period of time, a single sensor would likely only be able to observe a portion of it before the satellite exited its field of view. Observing the entirety of a long-duration manoeuvre may only be feasible for states and firms with far-reaching space surveillance networks. However, observing a portion of such a manoeuvre may be sufficient for validating the operator's claim about the capability being demonstrated.

Verifying Satellite Retirement

A satellite reaches the end of its operational lifetime by losing some or all of its subsystem-level capabilities, such as its ability to manoeuvre (propulsion), transmit and receive signals (communications), or recharge its batteries (power). Because a satellite operator may choose to let a satellite lie dormant – that is, remain capable of some or all of its original operations, but not make use of them for a prolonged period of time – and is not required by any particular obligation to declare retirements, the current operational status of any individual satellite is not perfectly understood by the satellite operator community or the public. This ambiguity poses challenges for threat assessment, particularly in congested orbital regimes where neighbouring operators and more distant third-party observers may fail to confidently distinguish between a controlled close approach by an active satellite and an untimely natural drift by a derelict one.

Under a new instrument of space security geared towards placing behavioural limits on operational satellites, states could make use of Verification 2.0 principles by declaring past dates on which each of their satellites retired or by treating an upcoming retirement manoeuvre as a coordinated demonstration of post-mission disposal. Third-party observers could choose to dedicate their space surveillance sensors to capture the moment of retirement to corroborate the declaration of intent or practise regular space object monitoring and take note of any activities by the satellite purported to have retired that would be incongruent with this status: a change of trajectory not possibly attributable to natural effects, a change in the satellite's orientation, or evidence of a radio-frequency emission, for example.

Such a proposal is actively being discussed at the EG-SSA due to its relevance for collision avoidance, because operators notified of an expected conjunction very much wish to know the manoeuvrability of the other object on a collision course with one of their satellites. The space safety benefits of this concept also extend past collision avoidance and into broader concepts of space sustainability. A retirement date for each satellite would allow for states to substantiate their adherence to the UN Guidelines for the Long-term Sustainability of Outer Space Activities, which allows them 25 years after the end of their operations to remove their satellites from popular orbital regimes, as first proposed by the Inter-agency Debris Coordination Committee's Space Debris Mitigation Guidelines.²⁰

²⁰ 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, UN, https://www.unoosa.org/documents/pdf/PromotingSpaceSustainability/Publication_Final_English_June2021.pdf; Inter-Agency Space Debris Coordination Committee (2024) *IADC Space Debris Mitigation Guidelines*, IADC-02-01, rev. 4, January, https://www.iadc-home.org/documents_public/file_down/id/5836.

Distinguishing Nominal from Anomalous Satellite Behaviour

States' concerns about certain satellite activities they observe in space may be driven by these satellites behaving in ways that deviate from their own past behaviours. If a satellite has deviated from its nominal behavioural mode before, it may well do so again. In some contexts, unpredictability may render a satellite threatening to other states.

To better mitigate such unpredictability, satellite operators could share information about what nominal operations look like for their fleets. For example, in addition to publishing descriptions of their current orbital trajectories, satellite operators could also share the orbital elements of the nominal orbit they use for station-keeping: that is, the orbit that they strive to keep using relatively frequent, likely low-magnitude manoeuvres.²¹ As another example, satellite operators could publicly declare which ITU satellite network is currently protecting their operations in the RF spectrum. The declared network would include not just the frequency band or bands the satellite is actively using for RF emissions, but also others that third parties can expect them to potentially use in the future.

Independent observers can then characterise the activities of satellites they discern in orbit in light of a shared concept of nominal operations. Satellites that behave as purported would corroborate their declared baselines, while unexplained deviations – or anomalous activities – could serve as evidence for further investigations or substantiate a request for clarification or consultation.

Assessing Whether a Satellite Is Operating in a Military Capacity

A perennial conundrum in space threat assessment is the challenge of discerning when a satellite is operating in a military capacity, because many satellites are inherently dual-use and pursue activities that blur the boundary between military and civil or commercial space operations.²² However, an existing provision of international law offers states the opportunity to recognise when one or more of their satellites are operating in a military capacity and may, under some circumstances, enjoy additional freedoms not available to satellites operating in a non-military capacity. State operators could choose to make such a declaration public as part of an agreement supported by Verification 2.0 principles.

²¹ Remarks by a satellite operator (2026) at Stability at the Space-Nuclear Nexus, a private workshop co-hosted by the Secure World Foundation and the Carnegie Endowment for International Peace, Washington, DC, 29 January, during a session not held for attribution.

²² A.A. Ortega (2023) "Not a rose by any other name: Dual-use and dual-purpose space systems", *Lawfare*, 5 June, <https://www.lawfaremedia.org/article/not-a-rose-by-any-other-name-dual-use-and-dual-purpose-space-systems>.

Article 48 of the ITU Constitution allows member states to “retain their entire freedom with regard to military radio installations”.²³ While invoking Article 48, military satellite operators may choose to forgo the burdensome process of international coordination of the RF spectrum and operate without an ITU satellite network protecting their RF emissions from harmful interference. In an agreement under Verification 2.0, states could publicly announce their Article 48 invocations, as needed, as a complement to the practice of declaring which ITU satellite networks are being used by which satellites in their fleet. When independent observers detect operations that deviate from declared ITU networks, they could consult the public record of Article 48 invocations to further contextualise the discrepancy. When satellites deviate from their declared ITU networks without an invocation of Article 48, the unexplained discrepancy may provide the conditions for clarification or consultation.

In current practice, invocations of Article 48 are recorded privately at the ITU, despite multiple unsuccessful efforts by ITU member states to make the list public.²⁴ A new agreement for space security might ask states to disclose their invocations in a process entirely removed from the ITU, which would allow for inconsistencies to emerge between the public record and the list privately held at the ITU. However, without access to the ITU’s list, independent observers could not determine whether the public declarations were complete.

Assessing Whether a Satellite Is Hosting a Nuclear Weapon

Traditional SDA tools – optical, radar, and wideband radio sensors designed to discern satellites’ respective orbital trajectories, orientations, and RF emissions often from distances of hundreds or thousands of kilometres away – are not capable of verifying Article IV of the OST and its ban on nuclear weapons in orbit. However, a recent study described a compelling concept of operation for new technology that could do just that.²⁵ A nuclear material detection device sized to meet the payload constraints of a small satellite in low-Earth orbit (LEO) could be capable of detecting nuclear material onboard other satellites when placed very near them for a prolonged period of time. Conducting such an operation safely would require consistent, high-quality sharing of both satellites’ orbital trajectories and agreement to strict behavioural limits during the period of close-distance inspection. Although third parties could independently observe these conditions, they could not make their own assessment of whether the target is hosting a nuclear weapon without access to the specialised detection capability or the data it collects. Whether this model embodies Verification 2.0

²³ ITU (1992) “Constitution and Convention of the International Telecommunication Union”, *Final Acts of the Additional Plenipotentiary Conference (Geneva, 1992)*, art. 48, <https://search.itu.int/history/HistoryDigitalCollectionDocLibrary/5.12.61.en.100.pdf>.

²⁴ Author interview with A. Vallet, Chief of Space Services Department, ITU Radiocommunication Bureau, 8 August 2023.

²⁵ A. Danagouliau (2026) “Verification of the Outer Space Treaty with cosmic protons”, *Nature*, 655(8123), 16 July: 585–590, <https://doi.org/10.1038/s41586-026-10783-2>.

therefore depends on how widely this capability proliferates and the practices with which the collected data becomes available outside of the parties involved in the inspection.

According to the new study, an inspector satellite could determine with confidence that a target satellite in LEO is or is not hosting a nuclear weapon by remaining within four kilometres of that target for one week.²⁶ But by the norms of space operations, such a small separation distance would demand the consent of the target satellite being inspected, because an uncoordinated close approach at this distance would likely be considered deeply concerning by the target satellite's operator. Past examples of uncoordinated close approaches in LEO – cases in which satellites' separation distance was as much as 40 times greater than what would be needed for detecting nuclear material – have been condemned by leading military space operators, who have cast such behaviour as “unusual and disturbing”.²⁷

The process would begin with a declaration: the state responsible for the target satellite, likely already bound by Article IV as a party to the OST, reiterates its commitment by explicitly declaring that the particular satellite does not host a nuclear weapon. A coordinated inspection designed to test that declaration could then proceed as follows. Before the inspector satellite performs a rendezvous with the target, both satellite operators begin sharing high-resolution orbital trajectory data for the satellites involved. The target satellite's operator agrees to refrain from conducting manoeuvres of any kind during the course of the inspection to mitigate the threat of collision. Because physical differences between the two satellites may cause their trajectories to diverge due to natural forces in the LEO environment, the inspector may need to manoeuvre over the course of the inspection to preserve the required inspection geometry. The details of those manoeuvres should be shared with the target's operator and assessed against its latest trajectory data. Other capable states could independently observe whether both satellites adhered to the agreed geometry and whether the target exercised the promised restraint, while the inspector's measurements would test the state's underlying declaration.

This kind of operation incorporates some elements of Verification 2.0, but only under certain circumstances. While third parties could verify that the inspection occurred under the declared conditions, they could not independently assess the target's nuclear status unless they also possessed the detection capability. If this capability remained confined to a single state or international

²⁶ Note: The proposal also described other operational concepts that could relax either of these two constraints. An inspector satellite could make its determination from a distance of more than four kilometres if it could maintain that relative position for much longer than one week. Similarly, if the inspector could maintain a separation distance less than four kilometres, it would need less than one week of detection time to make its determination. More than one inspector satellite working in tandem at close distances would also relax these constraints, allowing for greater separation distances and shorter times in position to reach their determination with the same level of confidence.

²⁷ W.J. Hennigan (2020) “Exclusive: Strange Russian spacecraft shadowing U.S. spy satellite, General says”, *Time*, 10 February, <https://time.com/5779315/russian-spacecraft-spy-satellite-space-force/>.

organisation and other stakeholders had to trust these findings, the operation would more closely resemble a conventional managed inspection. It would more fully exemplify Verification 2.0 only if multiple actors could replicate the inspection themselves or independently evaluate sufficiently complete data released by the inspector.

Conclusion

The outer space security concerns expressed by states in forums like the OEWG on PAROS are often more granular and contextualised than those that would be mitigated with a new categorical prohibition akin to Article IV of the OST. In this contemporary environment, a promising avenue may be new agreements that constrain satellite behaviour under particular circumstances, such as when their relative geometry creates operational advantages for attack, surveillance, or signals intelligence. Because the application of such limits would depend on how observed behaviour is interpreted, they are especially well suited to Verification 2.0, where competing assessments are grounded in a shared evidentiary basis.

Verification 2.0 does not require states to declare in advance every operational decision they intend to make when their satellites are in orbit, nor does it require them to share all of the knowledge they obtain from their investments in SDA technology. Instead, it offers a framework where states disclose enough information to make their declarations testable and share enough evidence to substantiate the concerns they feel about the behaviours of others.

Observing space activities from a distance will always be subject to measurement error. Satellite operators will likely continue to attempt to obscure their activities and develop new ways of doing so that are unforeseen today. Verification 2.0 would remain useful under these conditions because it does not require perfect certainty, but only enough declared information and observed evidence for multiple actors to independently assess claims about adherence.

Today, some spacefaring nations may place greater trust in what SDA technologies reveal about activities in orbit than in what other states say about their own operations. Verification 2.0 offers a special opportunity to bring these technologies into the diplomatic process as a means of managing such distrust.

Building Peace Together

Geneva Centre for Security Policy

Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
Contact: www.gcsp.ch/contact
www.gcsp.ch

ISBN: 978-2-88947-460-8



GCSP
Geneva Centre for
Security Policy