

**VCDNP**Vienna Center for Disarmament
and Non-Proliferation

Reducing Risk in Uncooperative Rendezvous and Proximity Operations

In September 2026, the VCDNP convened an intensive three-day working meeting between experts from ministries of foreign affairs, space commands, and the space industry. The group included companies leading the development of RPO and SSA capabilities, armed forces analysts from space intelligence centres, experts in space policy and regulation, and officials from both advanced and emerging spacefaring nations.

The group examined the security threats posed by uncooperative RPOs, scenarios in which they could trigger armed conflict, and what measures could be taken to reduce the risk of unintended escalation. This brief presents key outcomes from the workshop, providing States with expert-backed input for negotiations in the OEWG on PAROS and the UNGA First Committee.

What are Rendezvous and Proximity Operations?

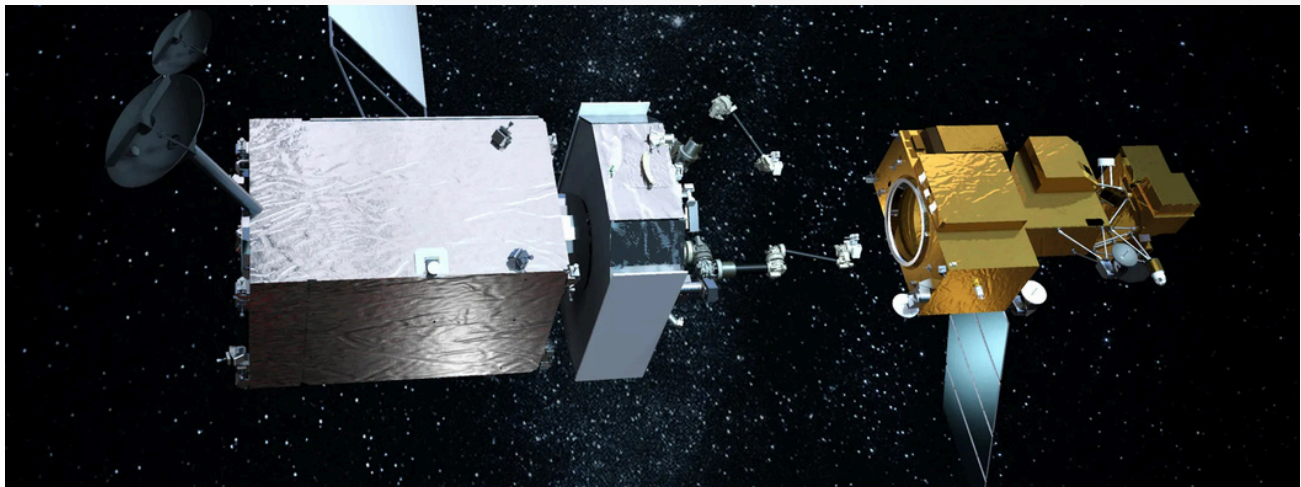
A **rendezvous** is a series of manoeuvres bringing two or more space objects very close together, matching their trajectories. They are often conducted to enable a physical connection through docking or berthing. **Proximity operations** are manoeuvres that place and keep a spacecraft near another object for some time to accomplish certain mission objectives.

The approaching spacecraft can be called **chaser**; the object being approached is the **target**.

RPOs have various commercial and defence applications:

- Rendezvous followed by docking or berthing can be used in on-orbit servicing and refuelling missions that extend a spacecraft's lifespan. They can be part of active debris removal missions that de-orbit inactive satellites or other debris. They are also routinely conducted in supply missions to the International Space Station (ISS).
- Proximity operations can be conducted for inspections, using cameras and sensors to understand a space object's dimensions and status in preparation for a servicing or removal mission. Similarly, they can be conducted to understand the capabilities of a spacecraft for military reconnaissance or to intercept signals exchanged between a satellite and ground stations for intelligence gathering.

While the basic capability has been used since the 1960s, RPOs are slated to occur more frequently. Life extension and debris removal missions may be deployed at scale to manage the growing amount of debris in the age of mega-constellations. And with domain awareness becoming the first priority in military competition in space, inspections of adversary assets are considered a key capability.



Concept of Northrup Grumman's OSAM-1 servicer grapple US government satellite Landsat 7 for refuelling. Credit: NASA

What are Uncooperative RPOs?

In **cooperative RPOs**, operators coordinate manoeuvres and share telemetry (battery voltage, temperature, fuel levels, etc.) and location data on their objects. To aid docking or grapple, the target may adjust its position and switch off its guidance, navigation, and control systems to prevent an accidental collision. Cooperative RPOs enable servicing and repair missions with key benefits for space sustainability and the peaceful uses of space.

In **uncooperative RPOs**, the target does not communicate its motion, orientation, or other data to aid the chaser. There is an important distinction between uncooperative RPOs conducted for in-orbit servicing and debris removal purposes and those conducted for defence purposes:

RPOs with defunct satellites or debris are uncooperative because the target *cannot* aid the chaser.

Such operations are conducted for in-orbit servicing or active debris removal missions being developed by a growing sector of the space industry. They contribute to the sustainable peaceful use of space. In many jurisdictions, these operations are subject to comprehensive licensing criteria that require safety by design and consent from the target owner.

Conducting an RPO with an active satellite without coordination is considered adversarial.

These operations can pose serious threats. They increase uncertainty in collision risk assessments as the target may be conducting station-keeping manoeuvres unforeseen to the chaser or may try to evade the approach. They can serve SIGINT purposes but may also be interpreted as preparation for hostile action, such as jamming, spoofing, or even kinetic attacks.



Commercial spacecraft designed for in-orbit servicing or debris removal are not capable of uncooperative RPOs with active satellites. There is a significant gulf in technical capability between commercial and military uncooperative RPOs.

Threats Posed by Uncooperative RPOs

States report an uptick in “unfriendly or even aggressive” RPOs targeting government and government-servicing satellites. The group of experts compiled key factors that increase the threat posed by an uncooperative RPO, building on real-world threat analyses in space commands and the spaceflight safety experience of industry experts. These factors include the capabilities of the chaser and the target, the chaser’s behaviour, the overall context, and any effects on the target.



A threat assessment can be triggered when a chaser changes to a trajectory that will place it close to a target or into a position from where little energy is needed to achieve proximity. An approach can be read differently depending on the orbital region. In LEO, fleeting conjunctions at high relative velocities are routine, so a slow, co-planar approach could signal hostile intent. In GEO, relative velocities are much lower, so a faster approach can signal a threat. If a chaser *matches* the target’s orbit, this is considered harassment and may be seen as preparation for attack.

Relations between the States involved are a major factor. An approach will also be seen as more dangerous if accompanied by an incident on Earth, for example, an attack on a ground station. The chaser’s RPO capabilities – whether it has thrusters and sensors to maintain proximity – and its payload are key for understanding which effects it could inflict. This is not public information but may be acquired through intelligence efforts. The target operator may examine the chaser’s previous movements to judge intent, for example, if the chaser often sits near communications satellites but does not otherwise interfere, it may be collecting SIGINT but pose an otherwise limited threat. The assessment will also depend on the capabilities and strategic value of the target: Can the target manoeuvre to evade the approach, are its transmissions encrypted, are other satellites available to provide continuity of service if there is interference, and is the target involved in nuclear deterrence?

How the chaser approaches is critical too: Is it using natural orbital dynamics to slowly drift towards the target along the GEO belt, visible to the target operator, or is it burning significant fuel to change its orbit, perhaps within a window when the target is not visible to ground-based tracking systems? The latter could result in the chaser suddenly appearing near the target in the next SSA data update available to the target operator. Exercises within space commands have shown that, with latency in SSA data, gaps in between when operators can programme new commands and manoeuvres, and insufficient communication from the chaser, pressure to manoeuvre pre-emptively rises. While the target may evade the chaser, doing so based on potentially outdated SSA data introduces more uncertainty and more safety risks.

Collision risk assessments shift with every change in trajectory, so calculations based on SSA data can quickly go out of date. On top of this uncertainty, operators use SSA data from different sources and of different quality. Depending on the assets involved, internal procedures, and varying risk tolerance, operators will draw different conclusions from that data – while the chaser operator may consider the approach safe, the target operator may see reason for a manoeuvre. These differences in interpretation contribute to risk during uncooperative RPOs.



The escalation risk of an uncooperative RPO is significantly higher if there are effects on the target. While RPOs for military reconnaissance and SIGINT gathering are increasingly tolerated as adversarial but not escalatory, any effects interfering with the normal and safe operation of the target in the context of an RPO are more likely to trigger a conflict.



Effects

- The chaser may jam or spoof the target's signal transmissions, interrupting service, or worse, disrupt or take over the telemetry, tracking, and control system of the target in a cyber attack.
- The chaser may dazzle or blind optical or infrared sensors aboard the target satellite.
- The chaser may deliberately collide with the target or release a sub-satellite or another deployable object that causes kinetic damage.
- Effects can even manifest after the chaser has manoeuvred away. The chaser could release a difficult-to-track object near the target, which may conduct a delayed attack, which would be difficult to attribute.
- Burning additional fuel to evade an approach shortens the target satellite's lifespan. This may be considered a more minor effect.

The following case studies show how seriously States can perceive threats posed by uncooperative RPOs and how they can contribute to arms race dynamics in space.

- **Luch/Olymp-K:** The Russian satellite Luch spent several years manoeuvring close to other communications satellites in GEO. In 2018, France reported that Luch had approached the Franco-Italian military communications satellite Athena-Fidus, alleging espionage. This incident prompted the development of a French space defence strategy and capabilities. While the original satellite has been deposited in a graveyard orbit, **Luch/Olymp-K 2** continues the same pattern. In 2025, Germany stated that both Luch satellites had been shadowing Intelsat satellites used by the German armed forces. The UK Space Command described Russian satellites following British assets. Across these cases, a core concern beyond SIGINT is the possibility of harmful interference or hostile action by the chaser.
- **Cosmos 2543:** In 2020, the Russian satellite Cosmos 2543, itself a separated sub-satellite, manoeuvred close to the US reconnaissance satellite USA 245 several times. The US Space Command called this behaviour "unusual and disturbing." Later that year, Cosmos 2543 released a projectile-like object, which US and UK officials characterised as a co-orbital ASAT weapon. A similar pattern of trailing or shadowing followed with Cosmos 2576 in 2024 and Cosmos 2588 in 2025, each placed in orbits closely matching US military Earth observation satellites.

Tools and Measures for Risk Reduction

States identify three main factors in uncooperative RPOs that contribute to escalation risk:

- 1. Operators struggle to identify the intent of an approaching satellite.** It can be difficult to determine whether an approach is unintentional – caused by imperfect SSA data, the natural perturbative forces that affect all satellites' trajectories, or legitimate manoeuvres to change a satellite's service coverage – or whether it is intentional and may pose a threat.
- 2. Information about the chaser is imperfect.** While some information like the chaser's previous movements can be gleaned from open sources, other information like its payload is not publicly available. The target operator may not know if the chaser is equipped with SIGINT capabilities – conducting adversarial operations but posing a limited threat to target – or whether it has laser or kinetic ASAT capabilities on board that could damage or destroy the target. This uncertainty invites worst-case assumptions.
- 3. Uncooperative RPOs pose a greater collision risk.** Without coordination, collision risk assessments carry greater uncertainty. This is exacerbated if the target manoeuvres to evade the chaser, and made worse if the chaser pursues the target. A collision resulting from an uncooperative RPO carries a higher risk of escalation and may be seen as an act of aggression.



Therefore, reducing risk in uncooperative RPOs can be achieved by creating ways to signal intent, enhancing available information, and protecting against collisions. The following are select measures that could be taken to reduce uncertainty and risk in each of these areas:



Signalling Intent

- **Operators conduct uncooperative RPOs in an observable fashion across at least 24 hours.** Operators can assuage concern about posing an ASAT threat by not using orbital plane changes in LEO, fuel-expensive drifts in GEO, or glare from the Sun for difficult-to-observe approaches. Readiness to shorten the chaser's lifespan by burning lots of fuel to approach faster can imply preparation for attack. Completing an approach in at least 24 hours gives the target operator time to observe, even across tracking blind spots, and reduces collision risk resulting from pre-emptive evasion manoeuvres.
- **Operators provide notifications and ephemeris data for manoeuvres that could affect conjunction assessments.** An ephemeris is a record of a spacecraft's time-stamped positions and velocities. Sharing ephemerides helps other operators to project the object's new trajectory and reduces uncertainty about why the object deviated from its expected trajectory, demonstrating due regard. Notifications could also include the manoeuvre time, expected orbital state, uncertainty or covariance, and an operational point of contact. This does not require disclosing the military purpose of the manoeuvre.
- **Satellites involved in uncooperative RPOs may 'squawk' to signal distress.** In aviation, signalling distress via air traffic control codes, defined by ICAO, is a standard practice in emergencies and security incidents. Similarly, satellites could emit omnidirectional radio-frequency signals to show distress or dissent with an uncooperative RPO. If the chaser proceeds, this may contribute to a more serious threat assessment.



Increasing Available Information

- **Launching States provide advance registration data on objects to be launched into space.** Because they do not yet have a pattern of life that can give clues about their purpose or intent, uncooperative RPOs conducted by newly launched objects can introduce greater uncertainty into threat assessments. Since there is no deadline for registration and since publication in the UN Register can take several months, sharing registration data before launch, e.g., via Art. XI OST, could reduce uncertainty and risk.
- **Launching States include spacecraft mass and size in the registration data.** Mass and size allow for limited conclusions about a spacecraft's capabilities. For example, larger spacecraft can produce more energy and host more capable payloads; this may include ASAT capabilities, such as lasers. In some cases, knowing mass and size may allow target operators to discount some of the threats that an approaching spacecraft may pose.
- **Launching States include information about objects intended for future separation in registration data.** In LTS Guideline A.5.8, States have agreed to include "the number and names of space objects that may, in the future, separate from the main space object". A key reason why the release of a deployable from the Russian sub-satellite Cosmos 2543 in 2020 triggered grave concern among other spacefaring nations is because this object was not included in the registration data.
- **States of Registry clarify the registration or non-registration of unidentified space objects if requested.** In LTS Guideline A.5.4, States have agreed to respond to enquiries "seeking clarification about the registration/non-registration of a space object that could presumably be under its jurisdiction and/or control". Knowing which State controls an approaching object is essential for threat assessments. Clarifying registration or control can even be in an adversary's interest, to avoid unintended consequences. If an 'unclaimed' spacecraft poses a credible threat, this may trigger defensive measures.



Protecting Against Collisions

- **In uncooperative RPOs, operators plan and follow passively safe trajectories at all times.** On a passively safe trajectory, the chaser does not pose a collision risk to the target even if the chaser lost propulsion, navigation, or control. This also protects against accidents caused by calculation error or imprecise SSA. This is already standard in the space industry; the servicer closes in on the client while flying safety ellipses around it.
- **Operators update the orbital parameters of released objects and enhance their visibility.** Smaller objects released in orbit, especially in GEO, may be difficult to observe. Operators should update the orbital parameters of released objects in the registration data and provide swift notification via Art. XI OST. Trackability can be enhanced through LEDs, retroreflectors, or coatings. Following LTS Guideline B.1.3, operators could also self-report the location of separated objects until distinguishable by ground-based tracking.



Highest-Risk Behaviours

There was consensus across experts from governments, space commands, and industry that certain behaviours in the context of RPOs are clearly escalatory and should be avoided during peacetime. While more can be identified, the group discussed two such behaviours in particular. Because the hostile intent behind these behaviours is unambiguous, States may find it feasible to adopt the following commitments:

- **Operators refrain from making physical contact with active satellites without consent.** Docking or berthing with an active satellite without consent and coordination is extremely dangerous, especially if the target attempts to evade. If contact is made, the guidance, navigation, and control system aboard the target would act out of control, likely resulting in a collision. This creates a serious risk of escalation.
- **Operators refrain from interfering with other satellites' telemetry, tracking, and control (TT&C) systems without consent.** Satellites and ground stations exchange two main types of data: *payload data* (like satellite imagery) and *TT&C data* (instructions from the ground and status information from the satellite). Interference with either is prohibited by the ITU Constitution and Radio Regulations. But while disrupting payload data may interrupt service to users, disrupting TT&C data cuts the lifeline between the satellite and its operator, leaving it unable to manoeuvre and vulnerable to collisions. This amounts to disabling the satellite and would likely be interpreted as an act of aggression.



Can 'exclusion zones' address threats posed by uncooperative RPOs?

UN forums often hear defined separation distances or 'exclusion zones' around satellites described as an effective risk reduction tool. However, operational experience shows that separation distance plays only a limited role:

1. **Spacecraft routinely come close to each other** due to normal orbital dynamics, especially in the populous low-Earth orbits and GEO. If one satellite maintains a safe trajectory in relation to another, posing no collision risk, it may not be perceived as a threat even if passing by at 3km in LEO. However, if one satellite aligns its trajectory to that of another, even at hundreds of kilometres' distance, operators will be alarmed.
2. **It cannot be defined at what distance an RPO take place.** The distance depends on the objective – reconnaissance with capable cameras and sensors can be conducted from tens of kilometres away; an inspection to prepare for in-orbit servicing will be done at a closer range.
3. **When a chaser may be 'too far away' to pose a threat depends on many factors**, such as the objective of the chaser, the capabilities of its payload, the strategic value of the target, etc. Some of these variables will be unknown to the target operator. Therefore, distance alone is a poor determinant of whether an approaching spacecraft poses a threat.
4. **'Exclusion zones' may be incompatible with international law**, specifically freedom of operation in Art. I and the non-appropriation of space in Art. II of the Outer Space Treaty.

Risk Reduction in the Existing Regulatory Framework

The group of experts considered how risk reduction measures around uncooperative RPOs fit into the existing framework of treaty obligations, UN guidelines, national regulations and policies, and industry best practices. The following are two of many examples that show how risk reduction measures can operationalise international law and build on standards for space operations created by armed forces and the space industry:

