Space Security Dialogue

Geneva, 3-4 July 2025
Chair's Summary

On 3 and 4 July 2025, the Geneva Centre for Security Policy (GCSP) held the second meeting of its track 2 Space Security Dialogue. This meeting summary has been prepared by the GCSP as Chair and represents their best efforts to capture the key recommendations from the dialogue and is not a consensus document.

General views

Overall, the experts believed that the key to achieving space security was through focusing on shared interests (and responsibilities) and reaching a common understanding of the threats to space systems. Transparency and verification should become standard principles of space governance. However, the lack of trust due to the geopolitical situation, was holding back efforts for an international data sharing framework and a space traffic management mechanism. Recent collisions and near misses should be a wake-up call, rather than waiting for something to go catastrophically wrong.

Inclusive dialogue that included all states (not just the major spacefaring ones), the commercial sector, think tanks, and scientific experts would help address threats to space security. Hard security issues (such as placement of weapons of mass destruction in space, initiatives such as Golden Dome, and the space/nuclear nexus) also needed addressing, but progress was more likely on less politicised topics such as data sharing and space traffic management.

During the dialogue, the experts discussed the following topics:

Defining the problem

The experts discussed what all space actors wanted to avoid. All stakeholders, states, and the commercial sector had a shared desire to prevent disruption to their space capabilities and denial of access to space. This meant no conflict in space and no attacks on space systems. Many highlighted the growing militarisation of space, with some states openly deploying weapons in orbit, and no longer masking military capabilities under dual-use pretences.

Traditionally, transparency was needed before you could begin discussing arms control, but this was difficult in the current context. Some wanted to see legal guarantees of responsible behaviour, given the difficulty of defining a space weapon. Others stressed the importance of understanding intent, as well as studying the second and third order effects of attacks on space systems. Many stressed the responsibility of the big three – China, Russia, and the US – if they agreed some rules of the road, that would cover 80% of space activity. Given the geopolitical context, scientific experts should be brought together to find technical solutions to these problems.

Space Situational Awareness: data sharing and trust-building in a geopolitically turbulent environment

All agreed that data sharing was crucial for space situational awareness (SSA). However, SSA capabilities were unevenly distributed, leaving significant blind spots in the tracking of objects in orbit. Limited SSA capabilities could make it possible for actors to evade detection while conducting hostile actions in orbit.

States should develop standards to ensure data quality and aid interoperability. Mechanisms, such as data hubs, could be developed nationally and regionally, to share information. The private sector could play a vital role in advancing the tools and methods necessary for improved tracking and coordination of space objects and offer tailored solutions. Trust-building exercises could be used to build confidence in 'trusted data'. Bilateral agreements could serve as early models for testing viable approaches.

In addition to an SSA framework, we needed a neutral, international space traffic management (STM) mechanism. It needed to be a collaboration between governments, the private sector, national bodies, and international bodies. The increase in in/on-orbit servicing would likely increase suspicions; hence the importance of transparency around proximity operations. A proposal based on one country's existing system was unlikely to be accepted, as it would disproportionately benefit that state politically and economically.

A mechanism whereby operators could speak to each other was needed. The recent conjunction incident between a Malaysian satellite and a North Korean satellite was mentioned as an example of operators finding it initially hard to communicate to address the problem.

Data sharing could be done at different levels of sensitivity, described as 'graded information sharing'. At the lowest level, one could have an orbital directory, then share data about uncertain measurements, then logs of manoeuvres, right up to sharing about planned future manoeuvres. The question was what the operators were willing to do and how much states were willing to compel them to do. Some queried whether such cooperation would be for all, or just for sharing amongst allies. Factors such as missile defence would always make sharing information about capabilities sensitive.

The era of mega-constellations: balancing between civilian benefits and military escalation

Mega-constellations raised several regulatory and military issues, such as dual use, collision risk, adequacy of the registration regime, increase in objects, and the impact on space traffic management. Some felt that there was a gap in the law, while others queried why mega-constellations were being discussed as a separate topic. They raised cross-cutting concerns, such as mega-constellations reducing access to space and their influence over military operations. Some said that the integration of artificial intelligence into STM systems raised concerns around oversight, accountability, and compliance with existing space law.

Others raised strategic stability concerns. The US was eyeing the development of Chinese mega-constellations with unease. If they were used in warfighting, there could be a military escalation risk, and the country of the commercial actor could be drawn into the war. Continuous and real-time surveillance through Ground

Moving Target Identification (GMTI) of an adversary would bring first nuclear strike advantages, calling into question the survivability of second-strike capabilities.

There were different views on civilian benefits; some stressed the connectivity they could bring to smaller countries, while others thought that any return on investment would take time, given the huge deployment costs.

Verification 2.0

The question of verification has been divisive for decades of space security discussions, with some arguing that it was not possible to verify whether a space asset was a weapon. We asked whether the combination of advances in technology and better information sharing could make it possible to verify certain types of weapon and behaviours.

Due to the increasing amount of publicly available data and observation capabilities, different means of verification were possible. For example, satellites could be assigned life cycle stages, where each stage indicates a predictable behavioural pattern. As a result, you could assign each satellite a certain stage, with attributes such as manoeuvring capability, intended orbit, intent analysis, and risk assessment.

However, tracking satellites still relied on the availability of data. Tracking sites could be biased, with some assets over-tracked, and others redacted. Registration information provided to the UN was often minimal. By analysing registrations, you could determine which categories of satellites could threaten you. You could also look at behaviours, for example lasering another satellite required prolonged line of sight.

Technological progress meant that the trend was moving more towards transparency, as it was becoming easier for all actors to observe the skies. Hiding aggressive conduct in space would become increasingly difficult.

The Space-Cyber nexus

Cyber-attacks on space systems were a critical area of concern. Such attacks were intended to deliberately destroy the entire functions of a mission, steal information, or deny access to a device. Commercial satellites, which were increasingly used for military purposes, often lacked the cybersecurity robustness of military satellites, creating systemic vulnerabilities. The advantages of such attacks for the perpetrators were the low costs, deniability, their non-physical nature and reversibility, and the difficulty of regulating them.

Given the fragmented nature of the space ecosystem, with multiple actors developing discrete components, the attack surface for cyber threats increased exponentially. A single system component could serve as a backdoor for adversaries.

Building resilience was key, as preventing attacks themselves was not possible. This included backup systems, mission continuity planning, and robust incident response protocols. Unfortunately, commercial entities often underreported cyberattacks to protect their reputations, limiting the collective ability to learn and adapt. It was crucial to share data on cyber-attacks globally to increase understanding and resilience for all actors.

Multilateral discussions of the nexus had been limited. There were some mentions in UN processes on information, communications, and technology (ICT), likewise, some in the UN processes on preventing an arms race in outer space (PAROS). However, what was really needed was a platform for discussion and sharing, for example a subgroup to the open-ended working group on PAROS in all its aspects. There also needed to be discussions around an agreement to prohibit cyber-attacks on nuclear command, control, and communications systems.

The role of small and medium sized spacefaring nations

New and aspiring space actors faced similar and different challenges to the big players. Whilst they wanted space to remain a global commons, they struggled with limited access to technology, legal knowledge gaps, and vulnerability to unequal partnerships. These states wanted to use space for commercial, social, and economic purposes. If space security became an issue, they would not be able to respond. To mitigate this, they needed norm building and to act together, through subregional, regional and cross-regional groupings.

Concerns were also raised about small countries being taken advantage of by big commercial actors. Large spacefaring nations were building spaceports in Africa and Latin America, creating dependency. Some states had not granted licences to Starlink, as they did not want to give up their sovereignty over domestic law.

Whilst space was still dominated by two or three big players, new actors were asserting themselves. For example, the Philippines partnered with Germany on the topic of due regard. It should also be recalled that the Global South made an important contribution to the adoption of the Outer Space Treaty.

Future discussions

Many felt that a track dedicated to dialogue with commercial operators was needed. Such a dialogue could focus on issues such as data sharing, space traffic management, and mega-constellations. It would need to include commercial actors from major spacefaring nations, as well as space security experts.

In addition to the commercial track, all agreed that the expert track should continue as well. The following topics were suggested for future discussions:

- Responding to a space crisis,
- Platforms for space cooperation (including lunar exploration),
- The risk and threats associated with the increase in on/in orbit servicing,
- Placement of weapons in space (including weapons of mass destruction),
- Space/Nuclear nexus (including NC3), and
- Missile Defence and Space Security.