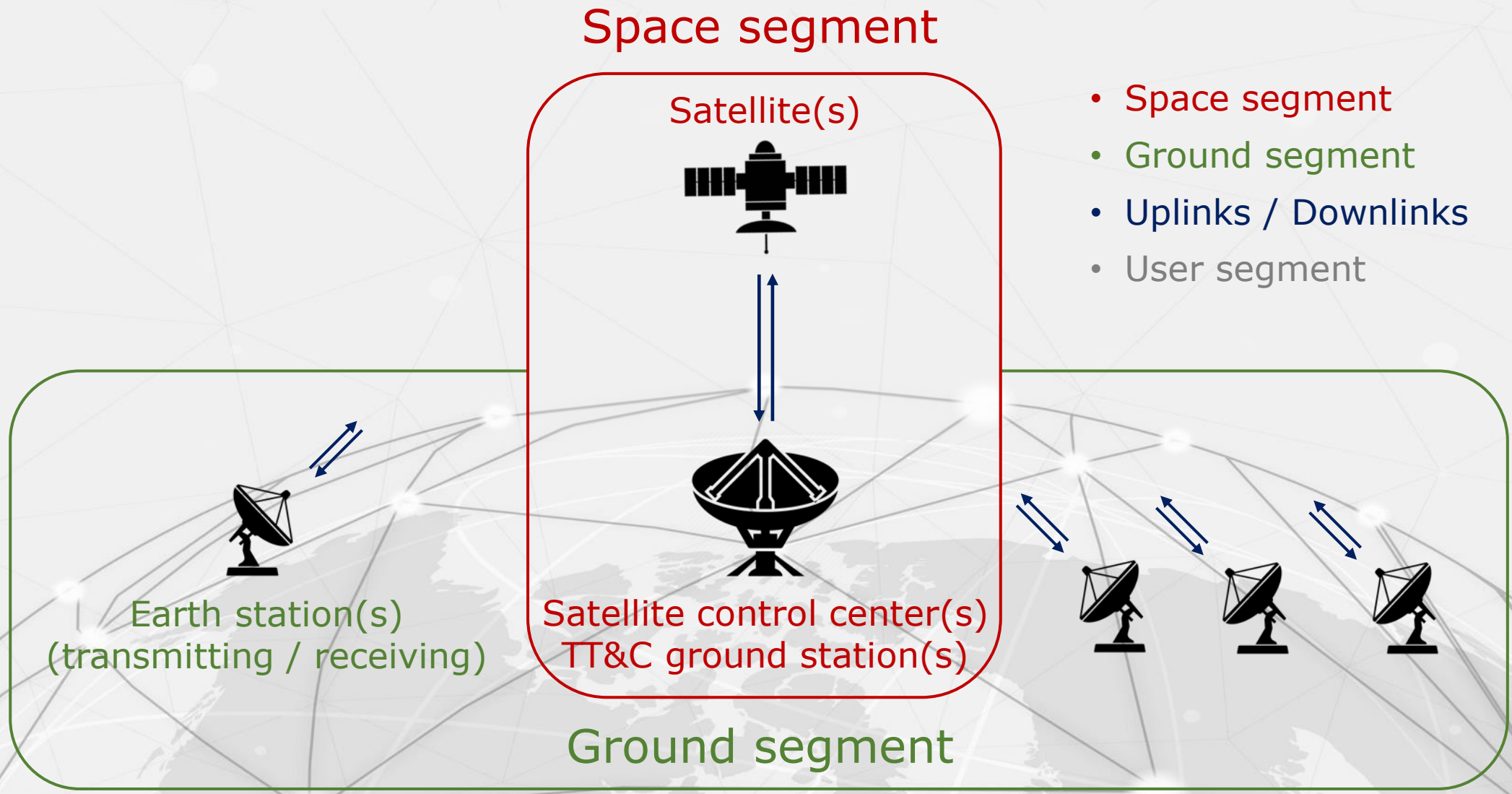
Current and future earth-to-earth threats by States to space systems

Open-ended working group on reducing space threats through norms, rules and principles of responsible behaviours
Second session, 12-16 September 2022

Elina Morozova, Executive Director, Intersputnik
International Organization of Space Communications

Segments of space systems



- Space segment
- Ground segment
- Uplinks / Downlinks
- User segment

Earth-based space infrastructure as a target

- Significant role of space systems in everyday life on Earth, incl. for critical space applications and commercial gain → space systems are a target *as a matter of when, not if*
  - Greater ease of attacking earth-based infrastructure compared to attacking spacecraft, no less great variety of impacts that can be caused
  - Complex supply chains for earth-based infrastructure and layers of stakeholders with different cybersecurity standards provide many opportunities for intrusion

Earth station(s)
(transmitting / receiving)

Satellite control center(s)
TT&C ground station(s)

Why cyber attacks ?

- Difficult to detect and investigate, and even more difficult to attribute
- Non-destructive (non-physical) and reversible damage, yet with no less powerful impact
- Cyber equipment accessible at low cost
- The use of traditional hardware and software by space systems familiar to attackers

Achieving a malicious goal with relatively little effort without being held accountable

What cyber attacks ?

Sensitive data, incl. personal data

Early warning systems, nuclear deterrence

Data from Earth observation satellites used in agriculture → improper crop care and reduced yields, leading to shortages and rising prices, disease and hunger

Smart cities: electrical networks, plumbing, transport systems are prone to failures

- ❑ Stealing / deleting / altering data
- ❑ Disabling operations temporarily / permanently
- ❑ Hijacking control over spacecraft

Demand a ransom

Causing harm to a hijacked satellite, e.g. by burning solar panels or deorbiting

Causing collision with another satellite and generating space debris

Responsibility for such activity in space and / or liability for damage may be borne by appropriate / launching states

The changing landscape: technological and operational aspects

- ***New architecture*** of space systems
  - *Multi-satellite systems*, i.e. large and very large constellations consisting of as much as hundreds of thousands of satellites
  - Transition to *line production* using off-the-shelf technology and *modular systems* with plug-and-play elements
  - *Miniaturization and simplification* of space technology, including by abandoning what is secondary (or recklessly considered secondary)
- ***Digitization*** of space systems
  - Replacement of unique analog technologies with more standard *digital solutions* of larger manufacturers, flexible and programmable payloads
- ***Rising connection*** between space systems and the earth domain
  - Growing number of *connected devices*, increasing integration of space systems into on-Earth applications (Big Data, IoT, M2M, AR/VR)

The changing landscape: new players and market conditions

Lack of cybersecurity standards for commercial entities nationally and internationally → ensuring cybersecurity falls to companies

- *Growing competition* in the space industry → focus on speeding up production and cost reduction
- *Decreasing cost* of manufacturing space technology and launch prices → access to space is more affordable
- *Increasing number of space actors*, incl. private entities (some are newcomers with less knowledge and expertise in applicable regulations and / or limited budgets)
- Deeper involvement of *private sector*, incl. commercial entities serving the military's needs

Mitigating threats: operators' perspective

- Close watch on space systems' operations
  - Cyber hygiene control *(incl. human factors)*
  - Traffic control: timely threat detection and response
  - Spacecraft control: detection of strange behaviours to identify satellites compromised by intruders *(incl. as an element of Space Situational Awareness and Space Traffic Coordination)*
- Information sharing / analysis centers
  - Incentivizing reporting cases and sharing experience of investigations *(most cases are not disclosed due to reputational risks)*
  - Attracting expertise from different sectors *(e.g. banking known for a high level of cybersecurity)*
  - Issuing warnings about identified vulnerabilities and methods of dealing with them *(incl. to operators using compromised types of hardware and software)*
  - Working at the national, regional and international levels *(cyberthreats are a global problem)*

Mitigating threats: users' perspective

- ***Advanced architecture*** of space systems and services
  - Diversifying used satellite orbits, satellite constellations and satellites, and changing traffic paths → *critical services do not rely on a single payload / single service provider*
    - Verifying critical satellite data by analyzing data obtained by other means *(from ground-based measurement centers, airborne drones, etc.)*
      - Minimizing threats to critical civilian services, *incl. by taking into account other users of the satellite when loading satellite capacity*
        - Benefiting from space objects' registration *(specifying general function of space object)*

Mitigating threats: regulators' perspective

- Ensuring cybersecurity of ***critical infrastructure***
  - Inclusion of space systems, both space and ground segments, in the list of *critical infrastructure*
  - Establishing *requirements* related to critical infrastructure, incl. requirements for
    - *spacecraft manufacturers* throughout the entire life cycle from design to decommissioning
    - *manufacturers of hardware and software* used in space systems, including technical support
    - procurement and supply *chains*
    - *critical infrastructure facilities*, incl. location, construction, maintenance, supply of utility services, use of hardware and software, personnel

Mitigating threats: recalling Article VI of the Outer Space Treaty

- ***International responsibility*** for national activities in outer space, ***authorization and continuing supervision*** of the activities of non-governmental entities in outer space → *states adopt and implement space related* ***national legislation***
  - ***Timely adopting*** national legislation on space activities
  - Defining ***space activities*** in a reasonably broad manner
  - Incorporating ***cybersecurity requirements*** and ***critical infrastructure related requirements*** into the process of ***licensing*** space activities
- ***Incentivizing adherence*** to the highest standards of carrying out space activities, both nationally and internationally, to avoid "flag shopping"