Progetto Jean Monnet
"EU Space Policy, International Law, and Sustainability" (EUSPIL)

Cybertechnology and Outer Space Law: New Frontiers for Armed Conflicts

12 March 2025 | 09:30-11:30

Lecturer Prof. Claudia CINELLI
University of Pisa

Università degli Studi della Campania
Luigi Vanvitelli | Microsoft teams

Course: Cybertechnology and Armed Conflicts

Course Professors: Prof. Maria Chiara Vitucci &

Prof. Giorgia Bevilacqua

Contact person: c.campodonico2@studenti.unipi.it

Università di Pisa
Centro di Documentazione Europea di Pisa
Dipartimento Scienze Politiche Università di Pisa
Università degli Studi della Campania Luigi Vanvitelli
Co-funded by the European Union

What is outer space?

Outer space is the vast, mostly empty expanse beyond Earth's atmosphere, where there is little to no air, extremely low pressure, and extreme temperatures.

From a legal standpoint, there is no universally agreed legal definition of where outer space begins. The most commonly referenced boundary is the Kármán line (62 miles above sea level, where Earth's atmosphere becomes too thin to support conventional aviation.), but some countries and organizations use different altitudes.

What is outer space law?

A branch of international law governing activities in outer space.
The cornerstone of space law is the corupus iuris spatialis:

- The 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, 1967)
- The Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (Rescue Agreement, 1968)
- The Convention on International Liability for Damage Caused by Space Objects (Liability Convention, 1972)
- The Convention on Registration of Objects Launched into Outer Space (Registration Convention, 1975)
- The Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (Moon Agreement, 1979)

What is cyberspace?

Cyberspace refers to the virtual environment of digital networks where communication, data exchange, and online interactions take place. It includes the internet, computer systems, digital infrastructure, and online platforms used for communication, commerce, security, and governance. Cyberspace is intangible, borderless, and constantly evolving, making it a complex domain for regulation and security.

Cyberspace Law

There is no single, universally accepted international law governing cyberspace. Key legal efforts include:

- Budapest Convention on Cybercrime (2001): Addresses cybercrime and international cooperation.
- Tallinn Manual (2013 & 2017): Provides guidelines on applying international law to cyber warfare.
- EU Cybersecurity Strategy: Strengthens protection against cyber threats.

Peaceful use in outer space

The principle of peaceful use is embedded in Article IV of the OST, which prohibits the placement of nuclear weapons or any other weapons of mass destruction in orbit, on the Moon, or on any other celestial body. It also restricts the use of the Moon and other celestial bodies exclusively to peaceful purposes.

While peaceful is generally understood as "non-aggressive," it does not necessarily mean "non-military," since military technology can still be used for scientific research and other permitted activities in space.

For instance, military satellites used for communication, navigation, weather monitoring, and even reconnaissance are not considered a violation of the OST, as long as they do not involve hostile actions or weapons deployment. Additionally, international legal interpretations allow for self-defense measures under Article 51 of the UN Charter, though the specifics of how this applies to outer space remain a subject of legal and diplomatic debate.

Peaceful use in cyberspace

The concept of peaceful use in cyberspace aims to prevent conflict and promote cooperative, non-aggressive use of digital technologies and information networks. This principle draws inspiration from existing international law principles, particularly those governing peaceful uses of physical domains like outer space and maritime zones. It seeks to:

- Prevent cyber warfare
- Protect critical infrastructure
- Protecting personal data, privacy, and national digital sovereignty.
- Ensure international digital cooperation
- Minimize potential for cyber-based conflicts

Challenges in Application

- Dual-Use Technology
- Lack of a Global Treaty: lack of universal consensus on defining cyber aggression.
- Attribution Issues: difficulty in identifying cyberattack perpetrators.
- Conflicting National Interests: different views on cyber sovereignty.

Peaceful use

cyberspace & outer space

Both cyberspace and outer space share principles of peaceful use, emphasizing non-aggression, cooperation, and scientific progress. However, challenges remain in ensuring compliance and preventing their militarization in global conflicts.

	Outer Space	Cyberspace
Global Commons	No nation can claim ownership.	No single entity has full control.
Security Risks	Space assets vulnerable to attacks.	Networks and critical infrastructure at risk.
Dual-Use Tech	Space technology has both civil & military uses.	Cyber tools can be used for defense & offense.
Conflict Risks	Space militarization debates.	Cyber warfare & state-sponsored attacks.

EU Space Policy

Technological Sovereignty

- Developing autonomous launch capabilities
- Creating indigenous satellite navigation and earth observation systems
- Reducing reliance on non-European space infrastructure

Economic Development

- Promoting European space capabilities
- Creation of new industrial sectors: support for space sector startups and SMEs
- Enhancing economic competitiveness in the global space sector:

Scientific Research

Key Research Areas

- Earth observation
- Astrophysics
- Satellite communications

Through initiatives like Galileo and Copernicus, the EU ensures independent access to space-based services. Additionally, the EU Space Programme strengthens resilience against space threats, fosters sustainable space exploration, and supports economic growth by investing in cutting-edge space technologies. The EU also promotes responsible space behavior, working with international partners to establish regulations that prevent conflicts and ensure the peaceful use of outer space

EU Security & Defence

The European Union now considers space a critical operational domain, on par with land, sea, air, and cyber environments. It has become essential for military missions and operations, directly supporting the EU's common security and defence policy. The EU space strategy for security and defence is a key deliverable of the Strategic Compass, a plan of action to strengthen the EU’s security and defence policy by 2030.
The key pillars of the strategy are:

Improving understanding of space threats.

International Partnerships

Resilience and protection of EU space systems.

Increasing the use of space for security and defence purposes

Space threats

Recent hostile actions, such as destructive anti-satellite missile tests and cyberattacks on space infrastructure, highlight the vulnerabilities of critical systems that support European industries and services. These incidents, including Russia's 2021 missile test and 2022 cyberattack on Viasat, demonstrate the interconnectedness of space security, cyber threats and geopolitical tensions.

Satellite Hijacking

Jamming & Spoofing Attacks

AI & Autonomous System Manipulation

Malware & Backdoors

Ransomware Attacks

EU’s Strategy for integrating space and cybersecurity

The EU acknowledges the growing interconnection between space and cyber threats, as satellites and digital infrastructures are increasingly targeted by cyberattacks.

Key EU Initiatives:

- EU Cybersecurity Strategy: Strengthens protection of space-based services.
- EU Space Surveillance & Tracking (SST) Programme: Enhances resilience against debris and cyber intrusions.
- Strategic Compass (2030 Plan): Integrates space and cyber defense policies.