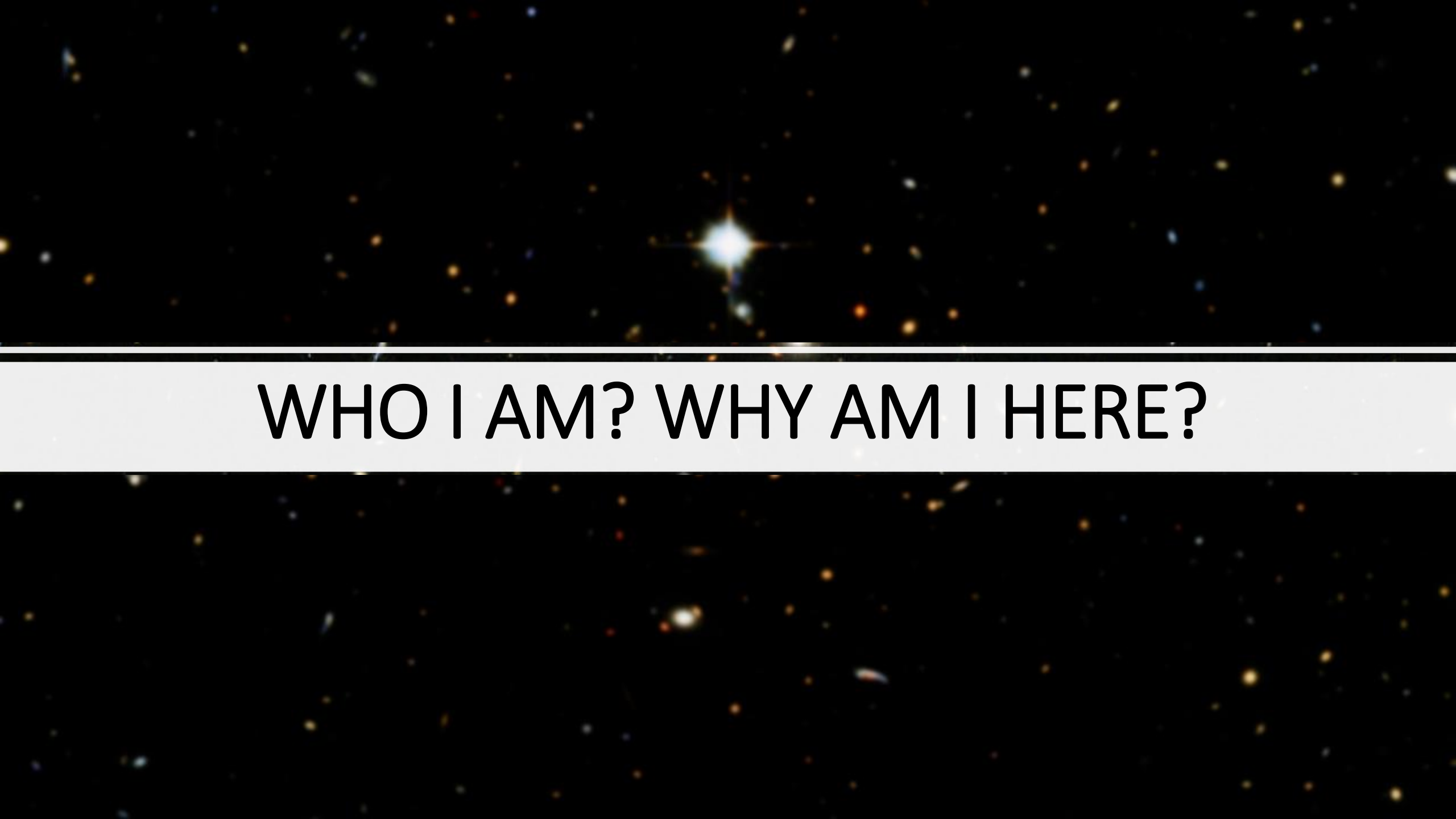
TROOPERS

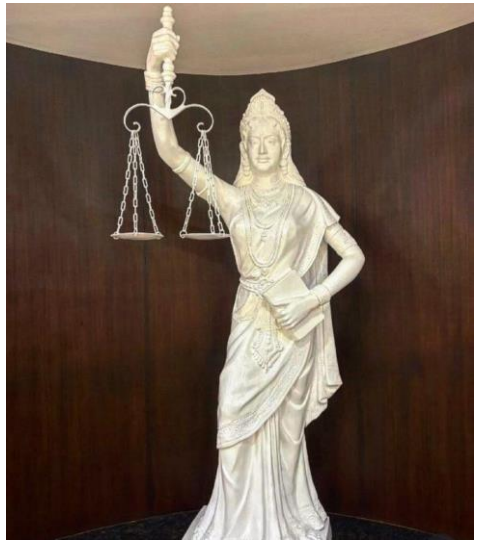
Space Security 101: A Legal and Policy Primer for the IT Community

RITANSHU LOHANI


WHO I AM? WHY AM I HERE?


काला हीरा
की धरती
धनबाद
में आपका
हार्दिक अभिनन्दन
THE BLACK
DIAMOND CITY
DHANBAD
WELCOMES
YOU


Google Earth
Data SIO, NOAA, U.S. Navy



ERASMUS MUNDUS JOINT MASTER

International Law of Global Security, Peace and Development

DISCLAIMER

This presentation is made in my personal capacity. The views expressed here are solely my own and do not reflect the positions or opinions of any institutions or organizations I am currently or have previously been affiliated with, including the United Nations Institute for Disarmament Research (UNIDIR) and the United Nations.

WHY SPACE MATTERS?

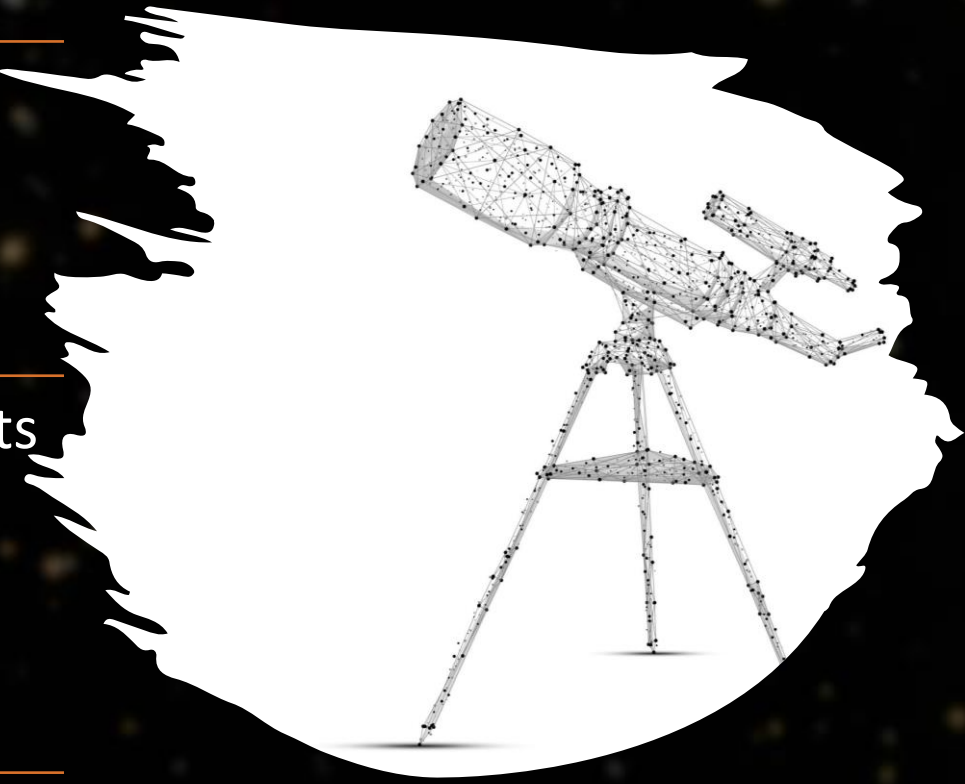
Source- United Office for Outer Space Affairs

WHAT EVEN IS *SPACE SECURITY?*

Commonly understood to refer to measures designed to prevent deliberate harms to a space system, including its component parts, from intended or intentional threats undertaken by another actor.

Concerned with the relationship between space objects and the maintenance of international peace and security (mitigation and prevention of threats), as well as the work of States to prevent an arms race in outer space.

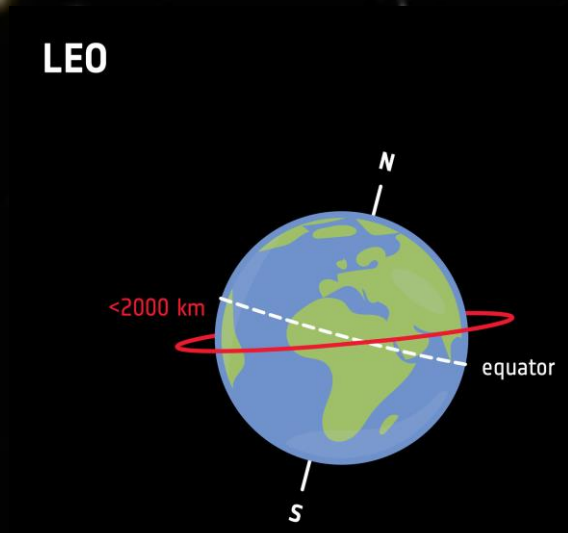
Discussions fall under the purview of the Conference on Disarmament, the UN General Assembly's First Committee, and the UN Disarmament Commission.

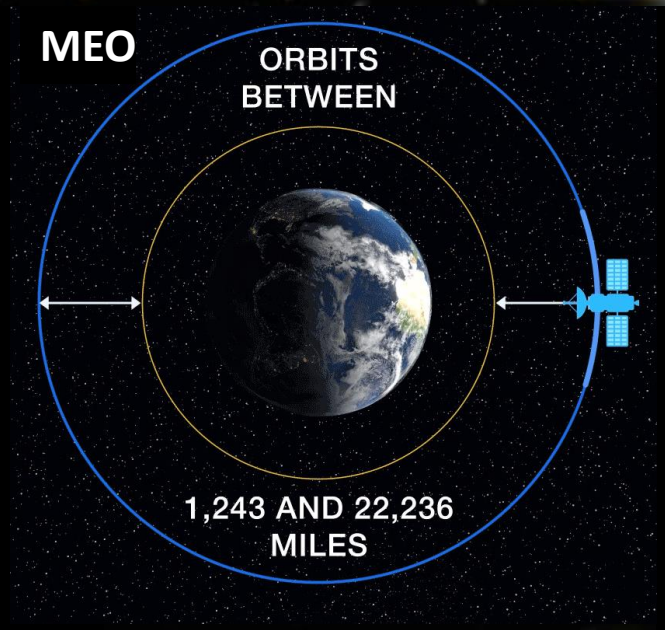


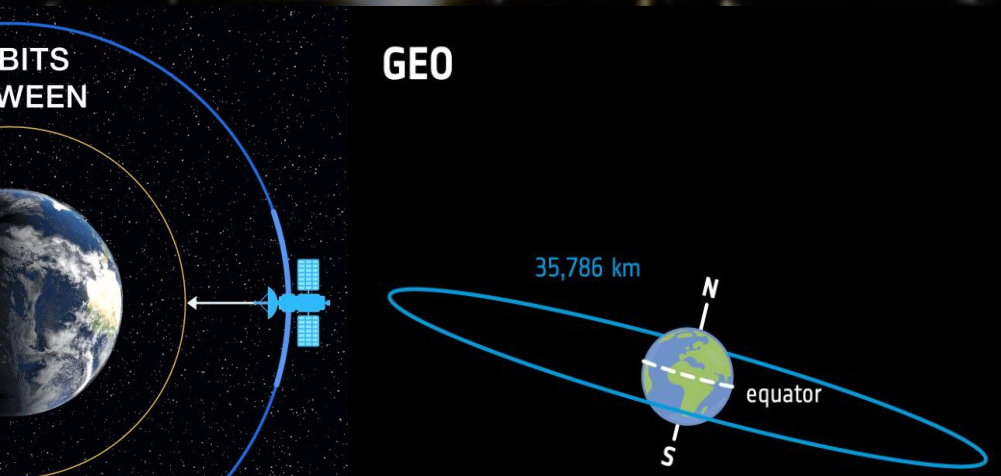
Source- UNIDIR, A Lexicon for Outer Space Security; Erickson. S 2023 "Current Trends and Developments in Outer Space Security, including Vectors of Threats".

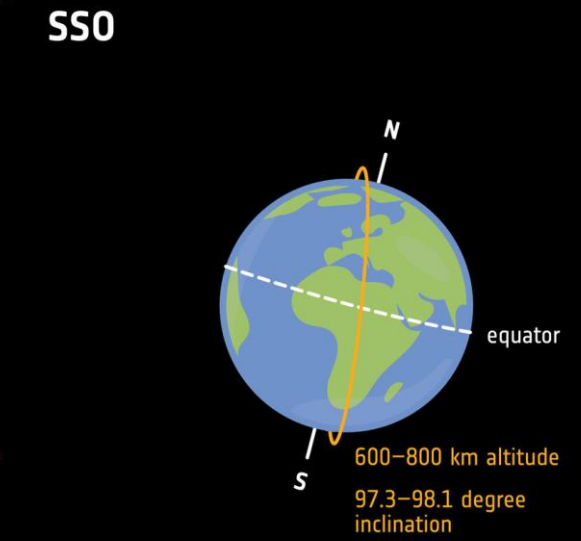

SPACE SECURITY ≠ SPACE SAFETY
9102-2917-9852-2116-3724
SPACE SECURITY + SPACE SAFETY = SPACE SUSTAINABILITY

TYPES OF ORBITS









Source- European Space Agency, 2020 and MEO picture from the US Space Force

SPACE SYSTEMS

Space Segment

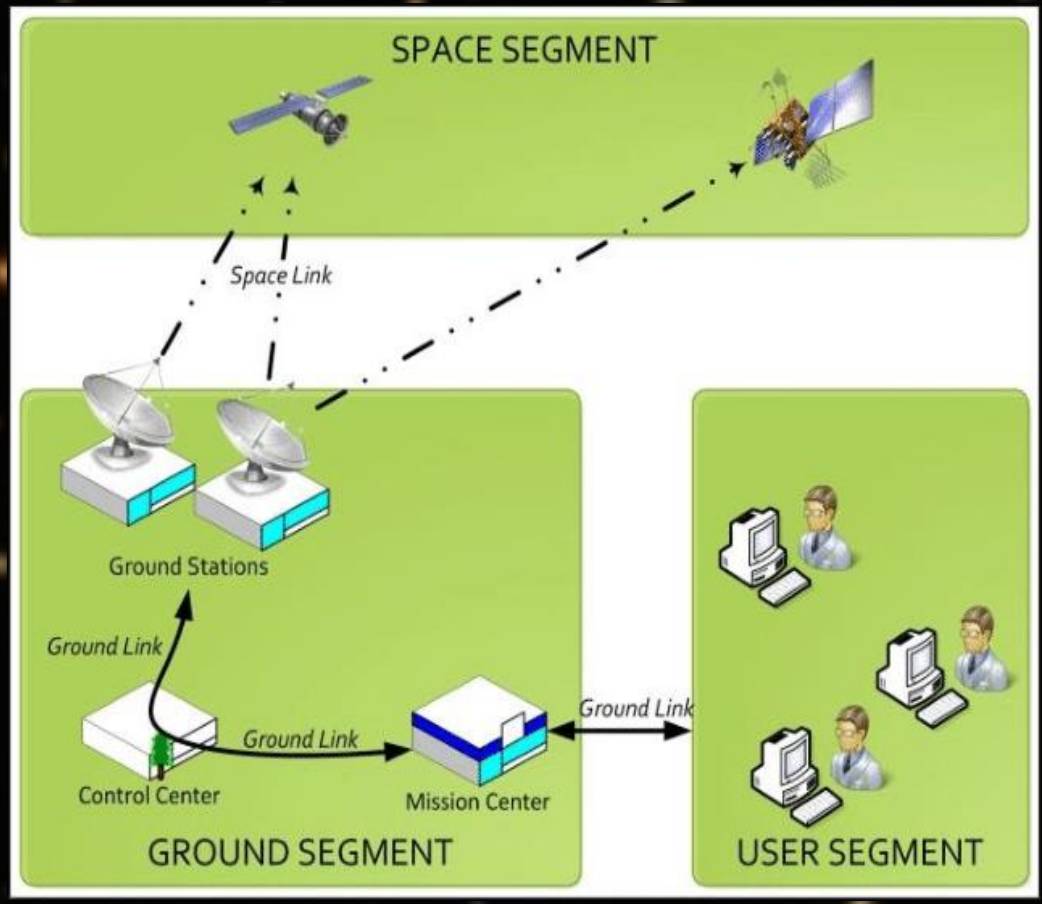
- any object launched into orbit from the Earth, the Moon, or other celestial bodies to travel to, in or through outer space
- includes component parts of a space object as well as its launch vehicle and parts thereof.
- Examples of space segment components are satellites and space launch vehicles.

Ground segment

- terrestrial part of a space system, which includes all the facilities and elements needed to operate a space object and deliver services to users.
- Examples of ground segment components include satellite dishes and receiving stations.

Data links

- the connection that shares information between the space and ground segments of a space system.
- includes the uplinks and downlinks, as well as services provided to the end users.



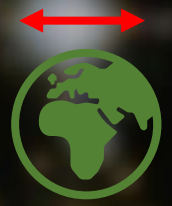
Source- UNIDIR, Space Security Lexicon (space segment, ground segment and data links)

Fig Source- Cerqueira, Christopher & Dos Santos, Walter & Ambrosio, Ana. (2013). Development of an Interface to a Spacecraft Simulator Empowered by Virtual Reality. SBC Journal on 3D Interactive Systems. 3. 37-44.

THREAT VECTORS

Earth-to-Space

- the targeting of space segments by capabilities and/or techniques which originate from Earth.



Space-to-Space

- the targeting of space segments by capabilities and/or techniques which originate from other space objects.

Space-to-Earth

- the targeting of assets located on Earth or within Earth's atmosphere by capabilities and/or techniques which originate from space.

Earth-to-Earth

- the targeting of ground segments by capabilities and/or techniques which originate from Earth.

Source: Spies. M 2024 "Developing approaches toward characterizing and verifying weapons in outer space"; Erickson. S 2023 "Current Trends and Developments in Outer Space Security, including Vectors of Threats".

SPACE THREATS

KINETIC PHYSICAL OR HARD-KILL*

- Direct ascent ASATs
- Co-orbital - ASATs, dual-purpose objects including RPO
- Ground station attacks
- Space-based anti-missile interceptors

NON-KINETIC OR SOFT KILL

Non-kinetic physical

- Electromagnetic pulse attack (including nuclear detonation)
- High-powered laser
- High-powered microwave

Electronic

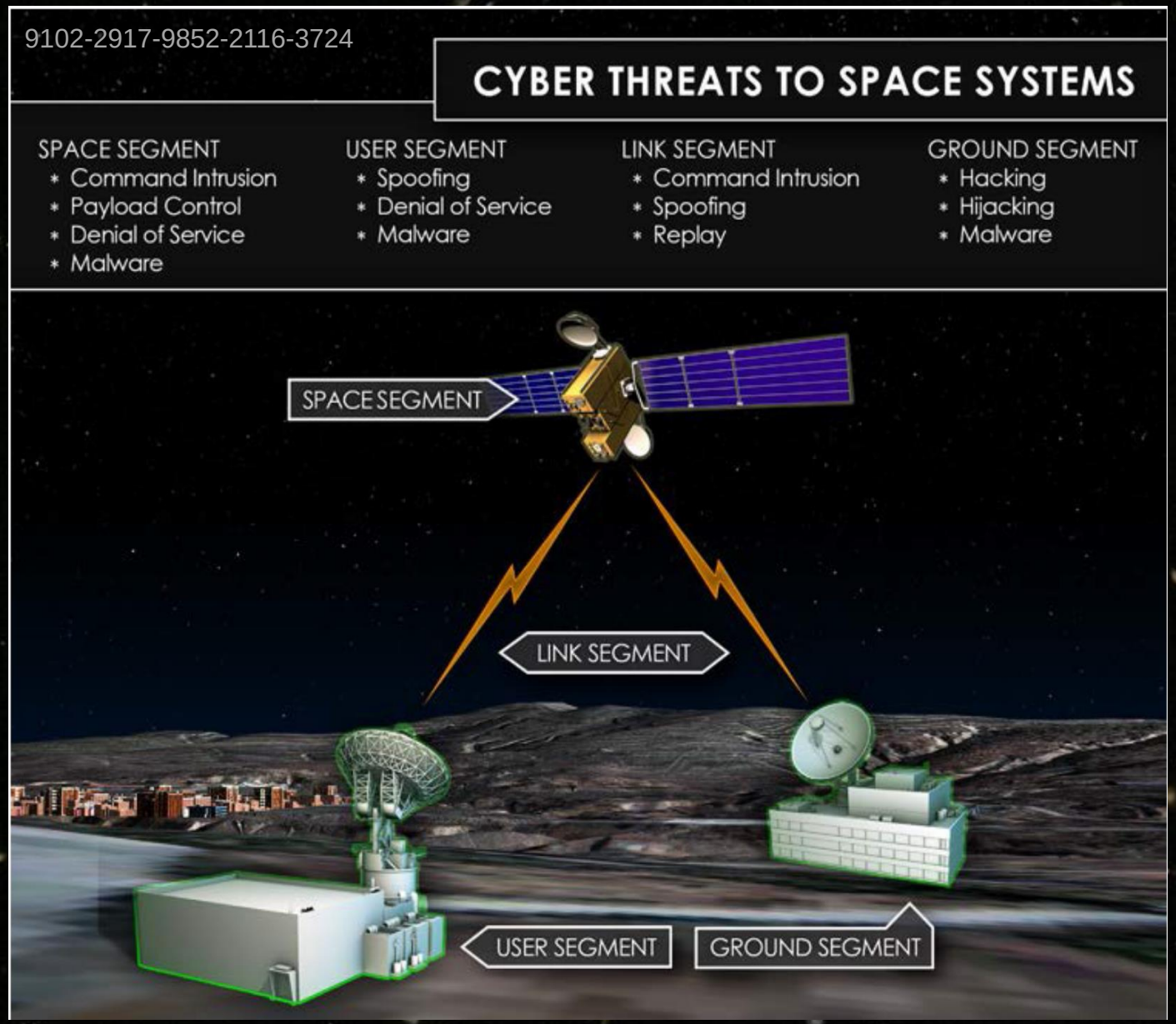
- Jamming
- Spoofing

Cyber

- Data intercept/monitoring
- Data corruption
- Seizure of control

MILITARY DOCTRINES/ NATIONAL LAWS AND POLICY

**any of these (except the interceptors) could use a nuclear warhead*

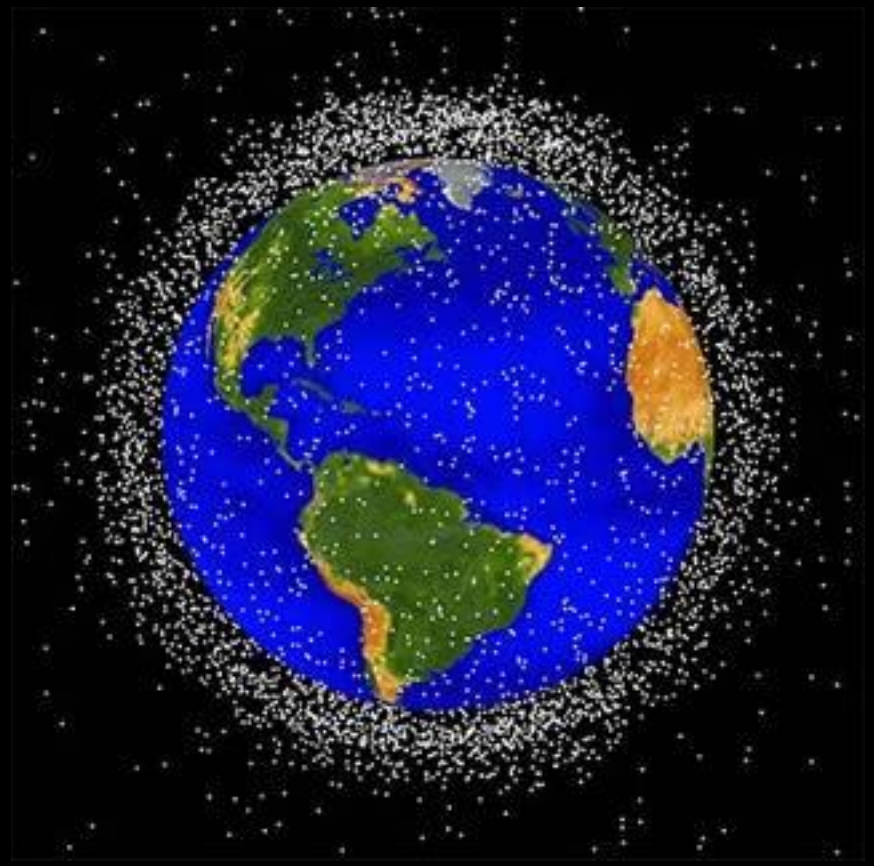


Source- National Air and Space Intelligence Center
Text Source- Secure World Foundation, Global Counterspace Capabilities Report 2025

CATEGORIES OF CYBER ATTACKS ON SPACE SYSTEMS

- Supply Chain Compromise
- Ground Segment Attacks
- Link Attacks (C2 / Data Links)
- User Segment Exploitation
- Satellite Compromise

SPACE DEBRIS



Pic source- NASA
GIF source- ESA

COUNTRIES' CAPABILITIES

	US	RUSSIA	CHINA	INDIA	AUS.	FRANCE	IRAN	ISRAEL	JAPAN	N. KOREA	S. KOREA	UK
LEO Direct Ascent	■	▲	▲	■	●	●	●	●	●	●	●	●
MEO/GEO Direct Ascent	■	■	■	●	●	●	●	●	●	●	●	●
LEO Co-Orbital	■	▲	▲	●	●	■	●	●	●	●	●	●
MEO/GEO Co-Orbital	■	■	■	●	●	■	●	●	●	●	●	●
Directed Energy	■	■	■	●	●	■	●	●	●	●	●	●
Electronic Warfare	▲	▲	▲	■	■	■	■	▲	■	■	●	●
Space Situational Awareness	▲	▲	▲	■	■	■	■	■	■	■	■	■

LEGEND: NONE ● SOME ■ SIGNIFICANT ▲ UNCERTAIN ? NO DATA –

Source- Secure World Foundation, Counterspace Capabilities Report 2025

INTERNATIONAL SPACE TREATIES

- Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (1967)
- Agreement on the Rescue of Astronauts, the Return of Astronauts, and the Return of Objects Launched into Outer Space (1968)
- Convention on International Liability for Damage Caused by Space Objects (1972)
- Convention on Registration of Objects Launched into Outer Space (1976)
- Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (1984)

Article I OST

"The exploration and use of outer space, including the Moon and other celestial bodies, shall be carried out **for the benefit and in the interests of all countries**, irrespective of their degree of economic or scientific development, and shall be the province of all mankind.

Outer space, including the Moon and other celestial bodies, shall be free for exploration and use by all States without discrimination of any kind, **on a basis of equality and in accordance with international law**, and there shall be free access to all areas of celestial bodies."

Article III OST

"States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the Moon and other celestial bodies, in accordance with **international law, including the Charter of the United Nations**, in the interest of maintaining international peace and security and promoting international cooperation and understanding."

Article 2(4) UN Charter

"All Members shall refrain in their international relations from the **threat or use of force** against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

Article 51 UN Charter

"Nothing in the present Charter shall impair the **inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations**, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

Article IV OST

"States Parties to the Treaty undertake **not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner**.

The **Moon and other celestial bodies** shall be used by all States Parties to the Treaty exclusively for **peaceful purposes**. The establishment of **military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manoeuvres on celestial bodies shall be forbidden**."

SPACE SECURITY APPROACHES

What to ban

- Capabilities
- Behaviours

How to ban

- Legally binding
- Non-legally binding

Source: Erickson. S 2023 "Current Trends and Developments in Outer Space Security, including Vectors of Threats".

WHAT CAN YOU DO?

Space Odyssey: An Experimental Software Security Analysis of Satellites

Johannes Willbold*, Moritz Schloegel*‡, Manuel Vögele*, Maximilian Gerhardt*,
Thorsten Holz‡, Ali Abbasi‡

*Ruhr University Bochum, firstname.lastname@rub.de
‡CISPA Helmholtz Center for Information Security, lastname@cispa.de

***Abstract*—Satellites are an essential aspect of our modern society and have contributed significantly to the way we live today, most notable through modern telecommunications, global positioning, and Earth observation. In recent years, and especially in the wake of the *New Space Era*, the number of satellite deployments has seen explosive growth. Despite its critical importance, little academic research has been conducted on satellite security and, in particular, on the security of onboard firmware. This lack likely stems from by now outdated assumptions on achieving security by obscurity, effectively preventing meaningful research on satellite firmware.**

In this paper, we first provide a taxonomy of threats against satellite firmware. We then conduct an experimental security analysis of three real-world satellite firmware images. We base our analysis on a set of real-world attacker models and find several security-critical vulnerabilities in all analyzed firmware images. The results of our experimental security assessment show that modern in-orbit satellites suffer from different software security vulnerabilities and often a lack of proper access protection mechanisms. They also underline the need to overcome prevailing but obsolete assumptions. To substantiate our observations, we also performed a survey of 19 professional satellite developers to obtain a comprehensive picture of the satellite security landscape.

***Index Terms*—satellites, satellite security, space segment, satellite firmware, threat taxonomy, software security**

in 2022 [2]. The vast majority of these satellites form mega-constellations like *Starlink*, which plans to launch more than 40,000 satellites in the coming years [3].

Small satellites [4] are at the heart of this *New Space Era* as their size and the widespread use of Commercial off-the-shelf (COTS) components makes them affordable even for small institutions. Furthermore, they cover a broad spectrum of use cases ranging from commercial applications (like Earth observation, machine-to-machine communication, and Internet services) to research applications, such as technology testing, weather and earthquake forecasting, and even interplanetary missions [5]–[8].

Although their applications vary wide
commonly consist of radio equipment ar
boards. Hence—in the broadest sense—t
systems connected to a ground station on
times, even to other satellites. Because the
connections for command and control a
trollers, they are potentially as vulnerable
other connected IT platform on Earth.

This issue has not been very relevant
access to ground stations was expensiv
large satellite operators. However, the
fundamentally in recent years. Nowaday
are even affordable for private individu
emergence of Ground Station as a Service
such as those offered by *Amazon Web*
Microsoft Azure [10], the entry barrier be
We have seen in the mobile network sec

iridium

MARKETS · TECHNOLOGY · INSIGHTS · SUPPORT · LOGIN

Vulnerability Disclosure Policy

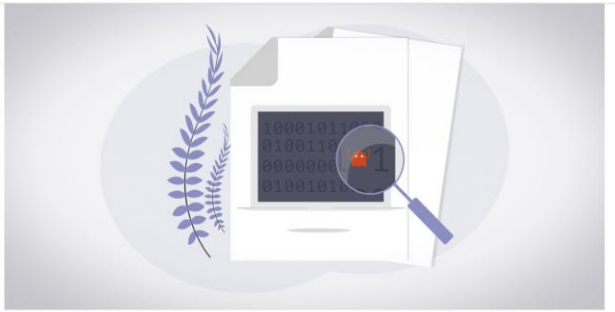
Introduction

This procedure is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to Iridium.

Explore | Search | News & Events | Multimedia | NASA+ LIVE

Home / Vulnerability Disclosure...

OCIO | Strategy Division | Cybersecurity and Privacy Division | Operations Division



Vulnerability Disclosure Policy

The NASA Mission is to drive advances in science, technology, aeronautics, and space exploration to enhance knowledge, education, innovation, economic vitality and stewardship of the Earth. A great deal of NASA work leverages information technology to capture, interpret, and appropriately share scientific knowledge to further its Missions and Programs. NASA is committed to protecting the confidentiality (where appropriate), integrity, and availability of its information and information systems.

NASA recognizes that external vulnerabilities can be discovered by anyone at any time and has issued this policy

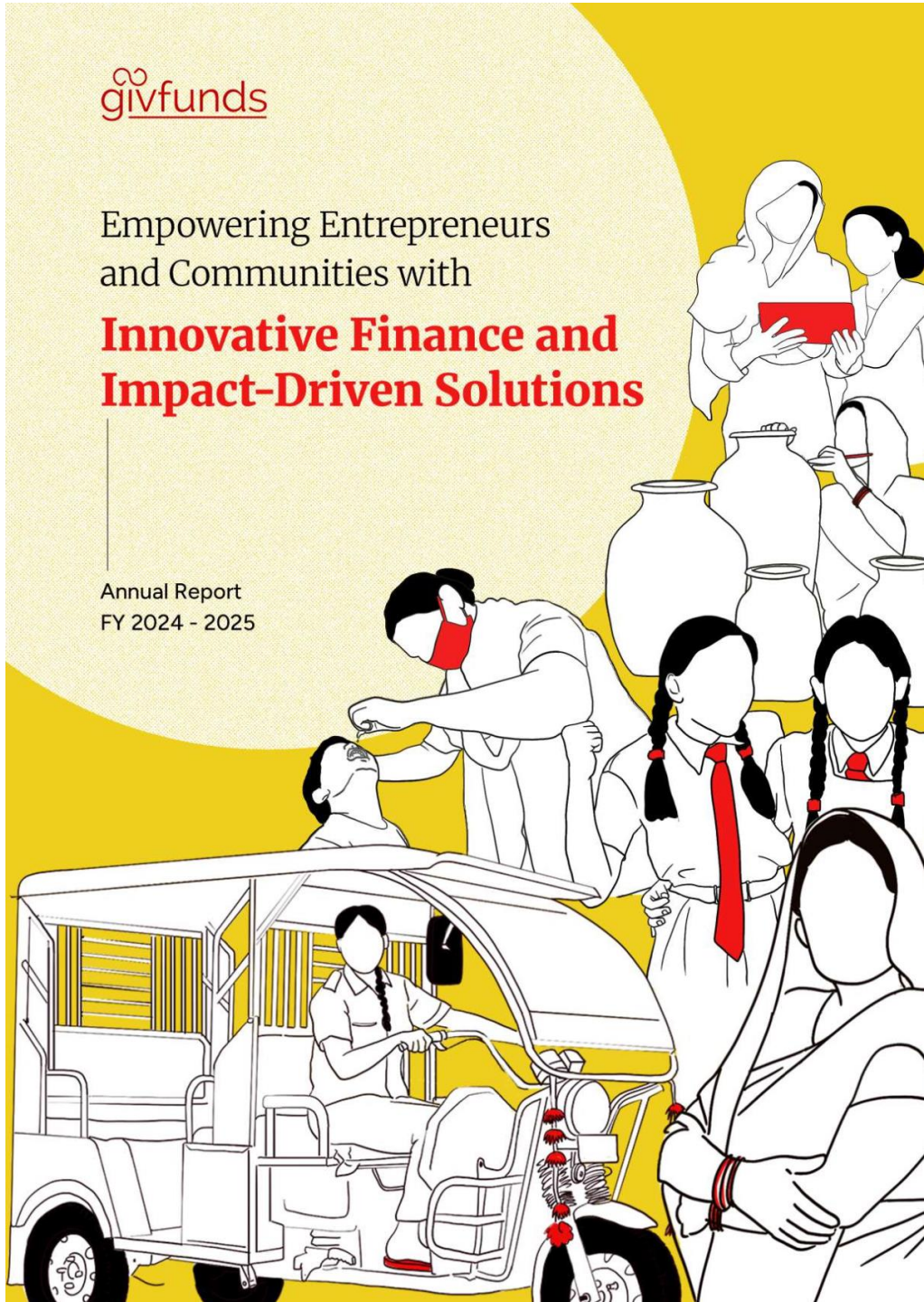
9102-2917-9852-2116-3724

Creating Ecosystem for Women Entrepreneurs through Innovative Finance & Capacity Building

Development Alternatives
People | Planet | Prosperity

givfunds

A collaborative effort by Development Alternatives and Givfunds



DONATION OF THE HONORARIUM

Source- givfunds

TROOPERS

Thank You!

Questions & Answers

ritanshulohani@gmail.com
/ritanshu-lohani