

CYBERSPACE SECURITY

LOW EARTH ORBIT

CHADI SALIBY



Background Image Source:
https://www.freepik.com/premium-photo/nightly-earth-planet-outer-space-with-sun-flare_40045770.htm

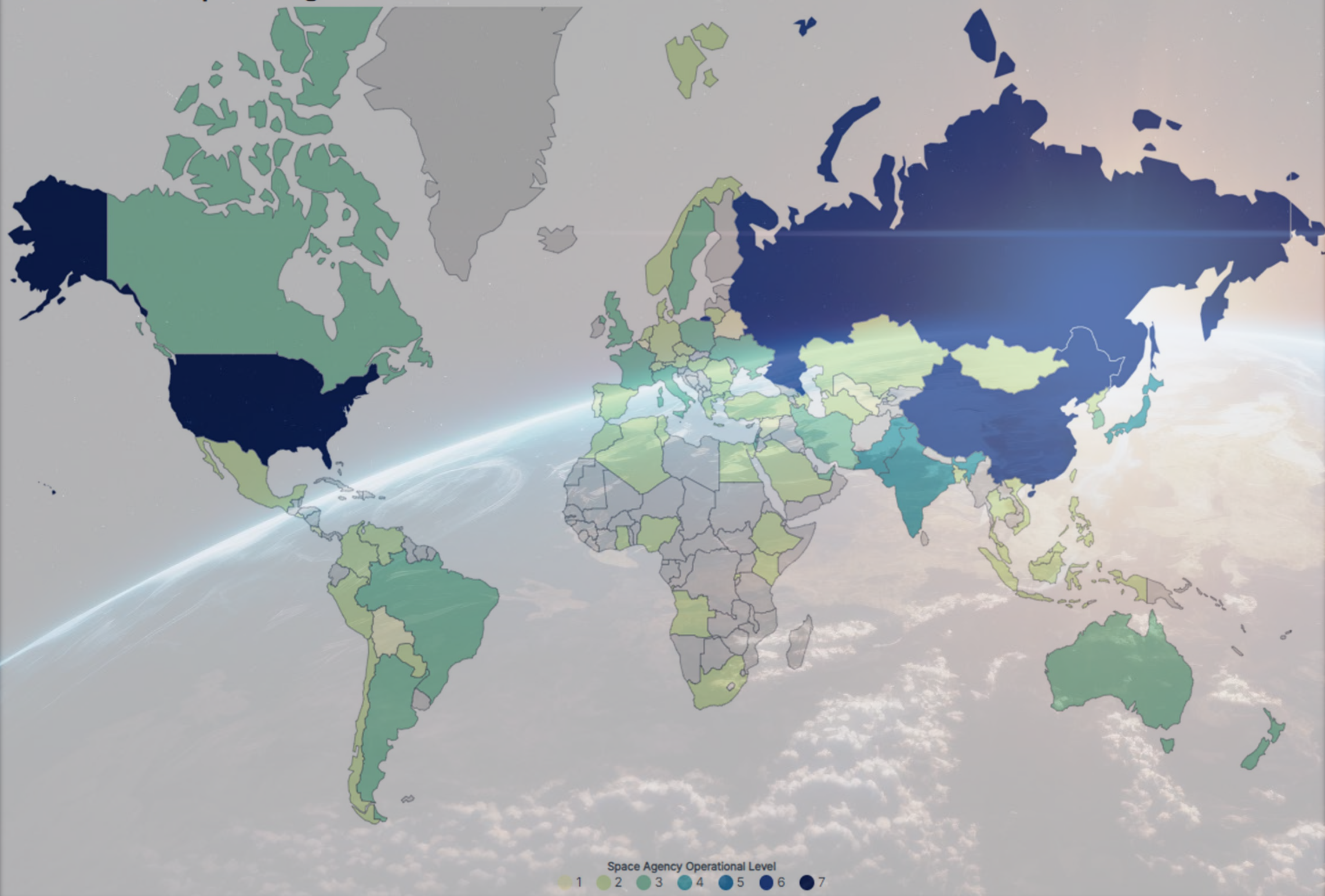
Critical cybersecurity challenges are emerging across low earth orbit (LEO) satellite networks, spanning both ground infrastructure and satellite platforms. This includes identifying key vulnerabilities, analyzing real-world case studies, and applying strategic best practices to safeguard space-based assets against an increasingly sophisticated and adaptive threat landscape.

- 🚀 Overview of common satellite architectures
- 🚀 Common cyberthreats to satellite systems
- 🚀 Vulnerabilities in ground control and satellites
- 🚀 Case study of past satellite cyberincidents
- 🚀 Strategies for hardening satellite cybersecurity
- 🚀 Emerging standards and regulatory considerations
- 🚀 Proof of concept and demo



Source: Pixabay. 2025. <https://pixabay.com/videos/planetspace-earth-satellite-nasa-145367/>

Countries with Space Programs 2025



Source: World Population Review. "Explore the World Population Through Data." worldpopulationreview.com, accessed July 2020



1U Standard
Dimensions:
10 cm × 10 cm × 11 cm

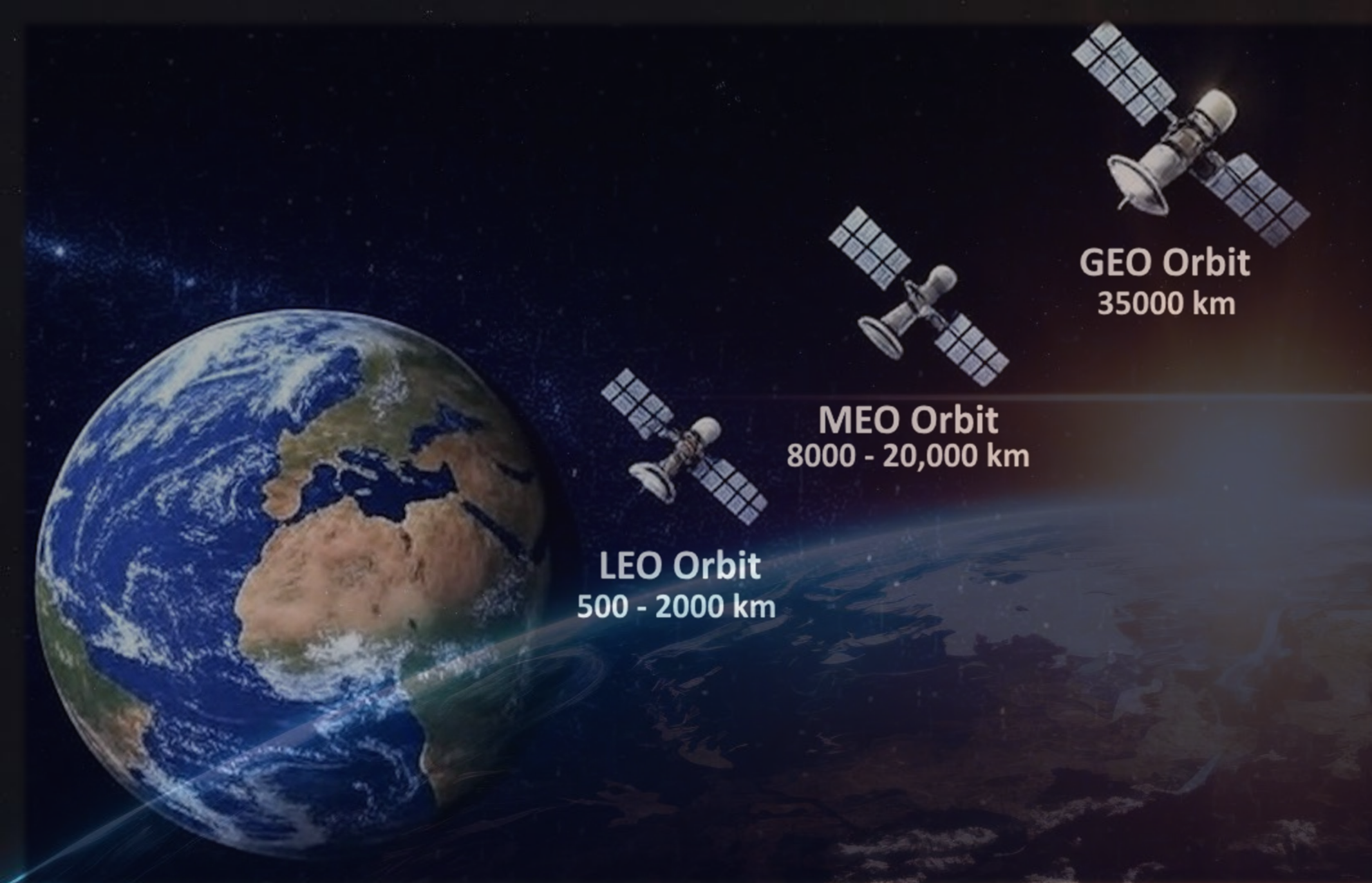
3U Standard
Dimensions:
10 cm × 10 cm × 34 cm

FIGURE 2: 1U CubeSat CP1 (left)
3U CubeSat CP10 (right) [Cal Poly]

Source: National Aeronautics and Space Administration (NASA). "CubeSat 101." https://www.nasa.gov/wp-content/uploads/2017/03/nasa_cslj_cubesat_101_508.pdf, October 2017.



IT'S ALL IN THE ATTITUDE



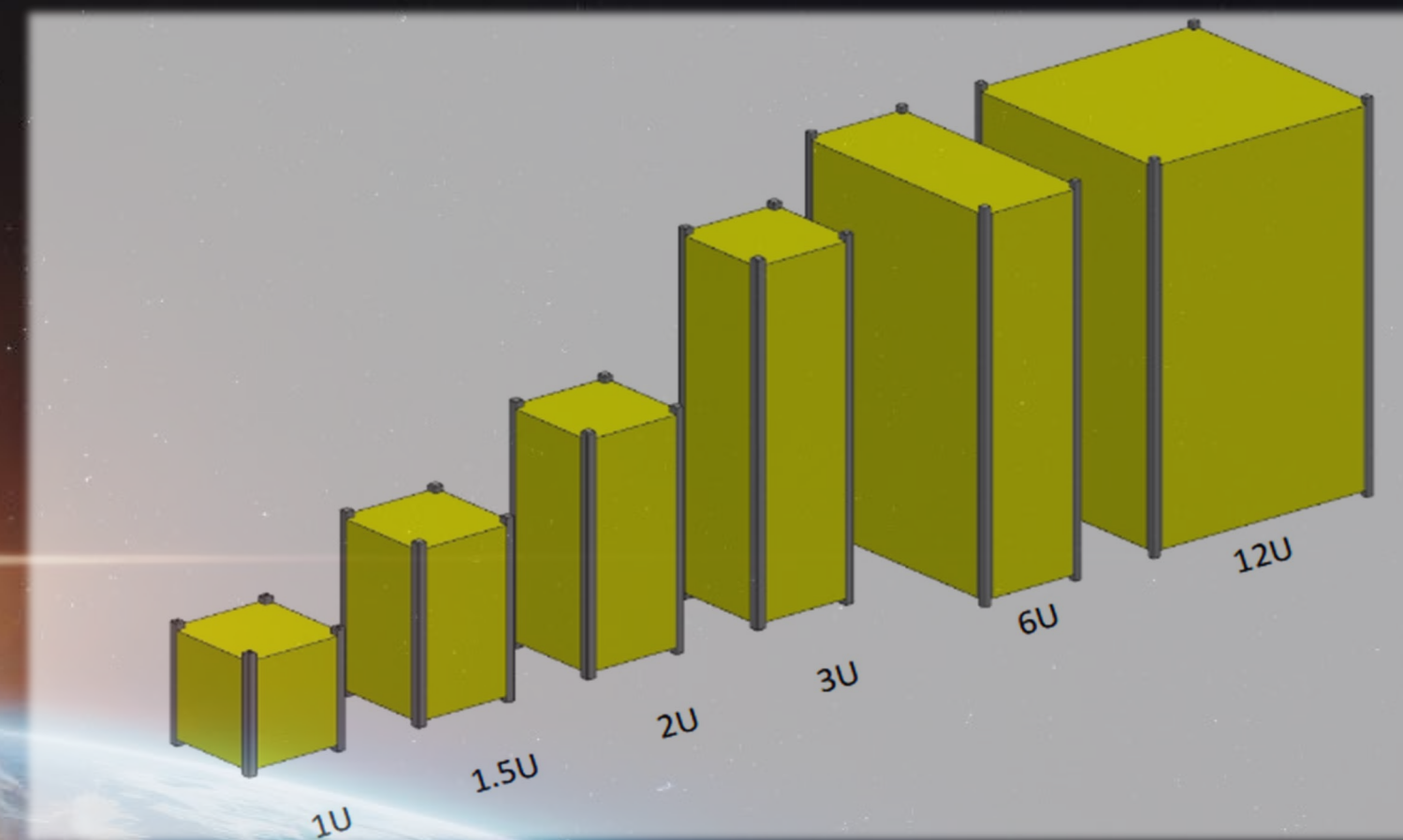
LEO Orbit
500 - 2000 km

MEO Orbit
8000 - 20,000 km

GEO Orbit
35000 km

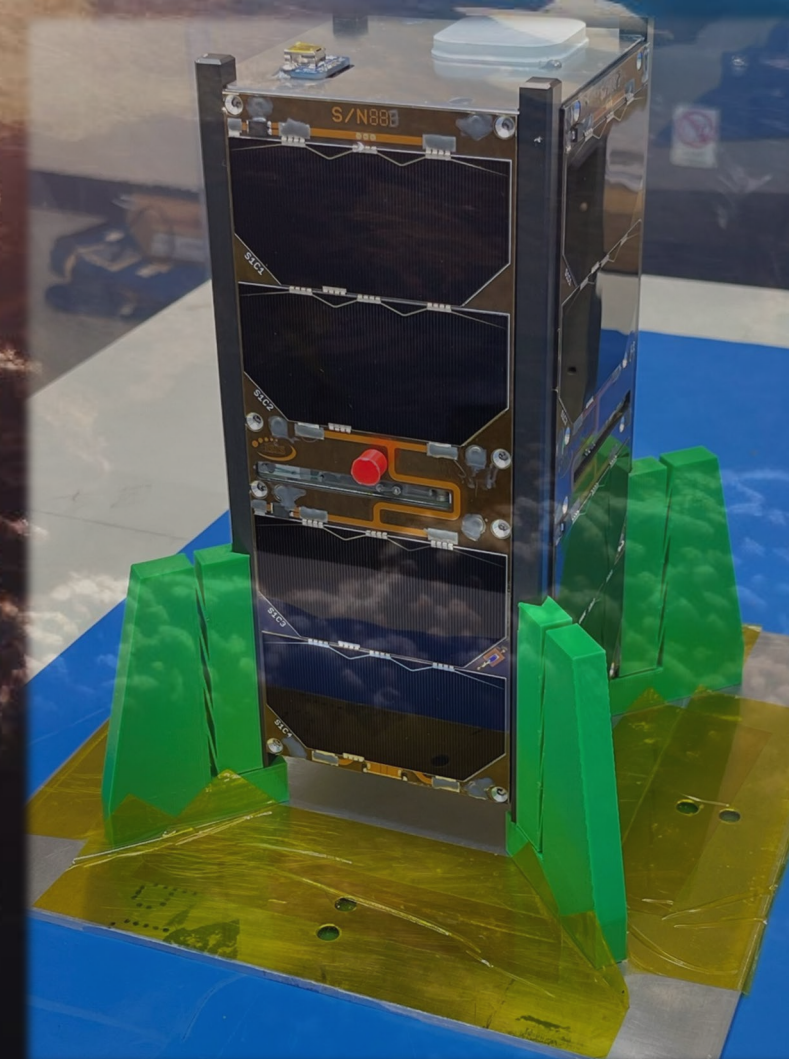
Note: GEO = geospatial earth orbit, MEO = medium earth orbit.
Source: Saliby, C. Edited using draw.io.

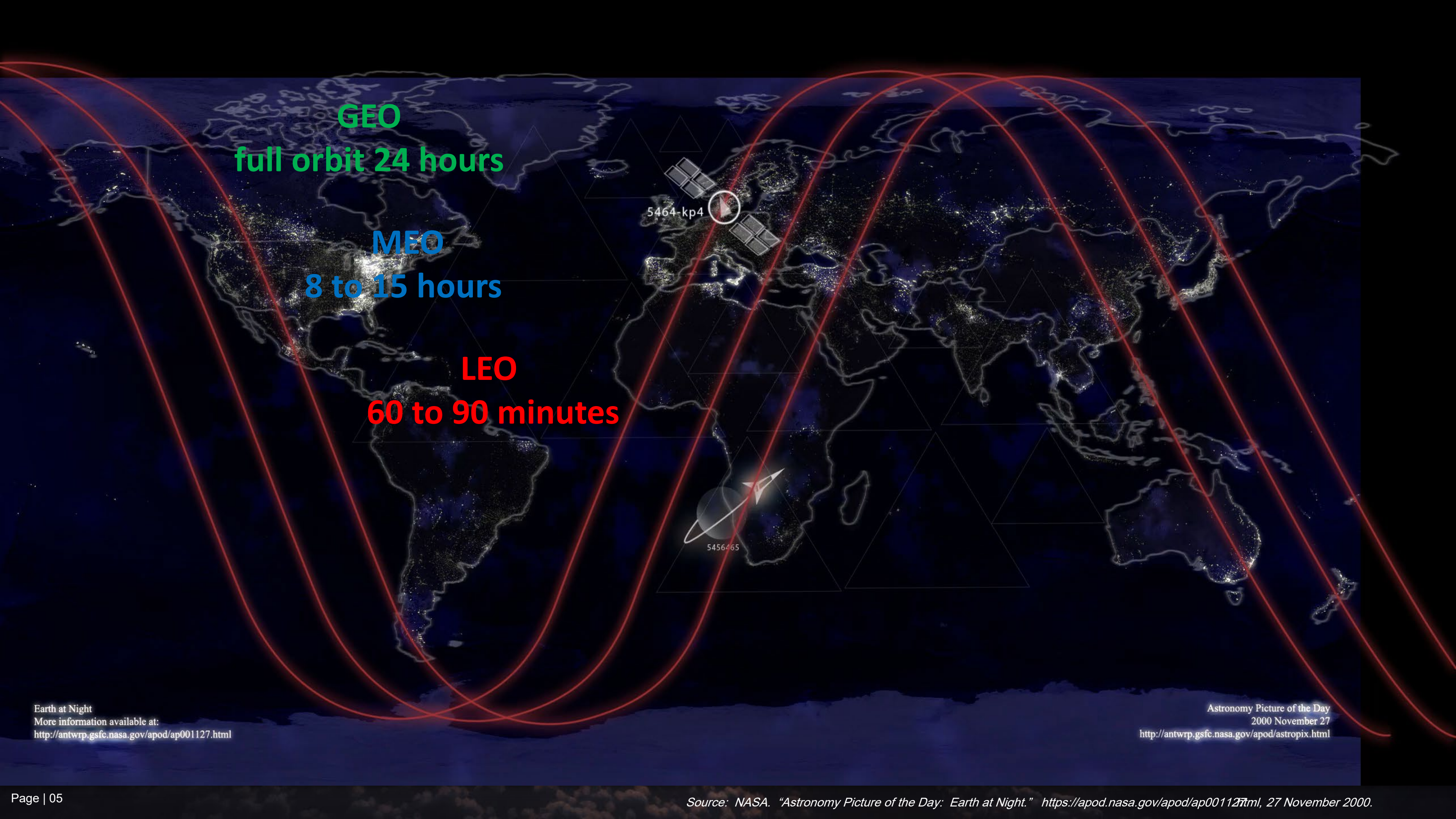
**TJREVERB CubeSat, by Thomas Jefferson
High School for Science and Technology**
2U CubeSat (10 cm × 10 cm × 22.7 cm)



U Configuration	Mass [kg]
1U	2.00
1.5U	3.00
2U	4.00
3U	6.00
6U	12.00
12U	24.00

Source: California Polytechnic State University, San Luis Obispo. The CubeSat Program." 2025.





GEO
full orbit 24 hours

MEO
8 to 15 hours

LEO
60 to 90 minutes

5464-kp4

5456465

Earth at Night
More information available at:
<http://antwrp.gsfc.nasa.gov/apod/ap001127.html>

Astronomy Picture of the Day
2000 November 27
<http://antwrp.gsfc.nasa.gov/apod/astropix.html>

AWS Ground Station

Easily control satellites and ingest data with fully managed Ground Station as a Service

Get started with AWS Ground Station

Introduction to AWS Ground Station

AWS Ground Station is a fully managed service that lets you control satellite communications, process data, and scale your operations without having to worry about building or managing your own ground station infrastructure. Satellites are used for a wide variety of use cases, including weather forecasting, surface imaging, communications, and video broadcasts. Ground stations form the core of global satellite networks. With AWS Ground Station, you have direct access to AWS services and the AWS Global Infrastructure including a low-latency global fiber network. For example, you can use Amazon S3 to store the downloaded data, Amazon Kinesis Data Streams for managing data ingestion from satellites, and Amazon SageMaker for building custom machine learning applications that apply to your data sets. You can save up to 80% on the cost of your ground station operations by paying only for the actual antenna time used, and relying on the global footprint of ground stations to download data when and where you need it. There are no long-term commitments, and you gain the ability to rapidly scale your satellite communications



Azure Orbital Ground Station

Current Selections

Date: All dates

Sort by: Newest to oldest

Refine results

Search

Product category

Audience

Content type

Date

Announcements · Dec 11, 2023 · 6 min read

Create new ways to serve your mission with Microsoft Azure Space >

As customers and partners have adopted and experimented with the Azure Space portfolio, new and interesting use cases are emerging that illustrate what's possible.

Announcements · Sep 11, 2023 · 6 min read

Accelerating the pace of innovation with Azure Space and our partners >

Together with our partners, we are rapidly innovating to provide every space operator with the solutions to solve persistent challenges in new ways and capture new opportunities in the rapidly expanding space sector.

Announcements · Apr 11, 2023 · 6 min read

Azure Space technologies advance digital transformation across government agencies >

Since its launch, Microsoft Azure Space has been committed to enabling people to achieve more, both on and off the planet. This mission has transcended various industries, including agriculture, finance, insurance, and healthcare.

Partnerships · Nov 17, 2022 · 7 min read

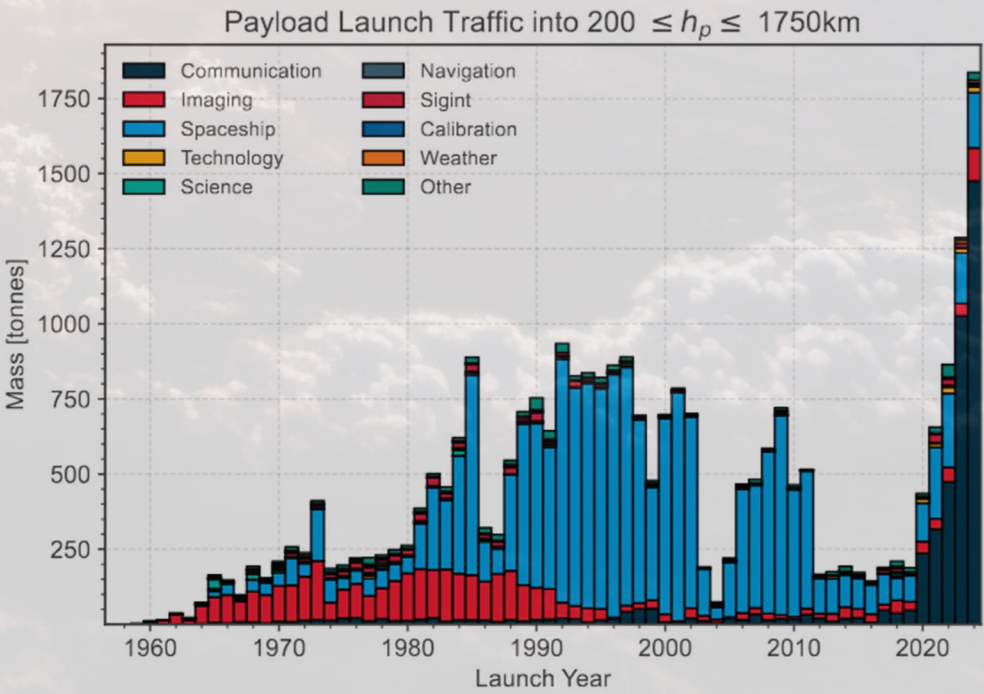
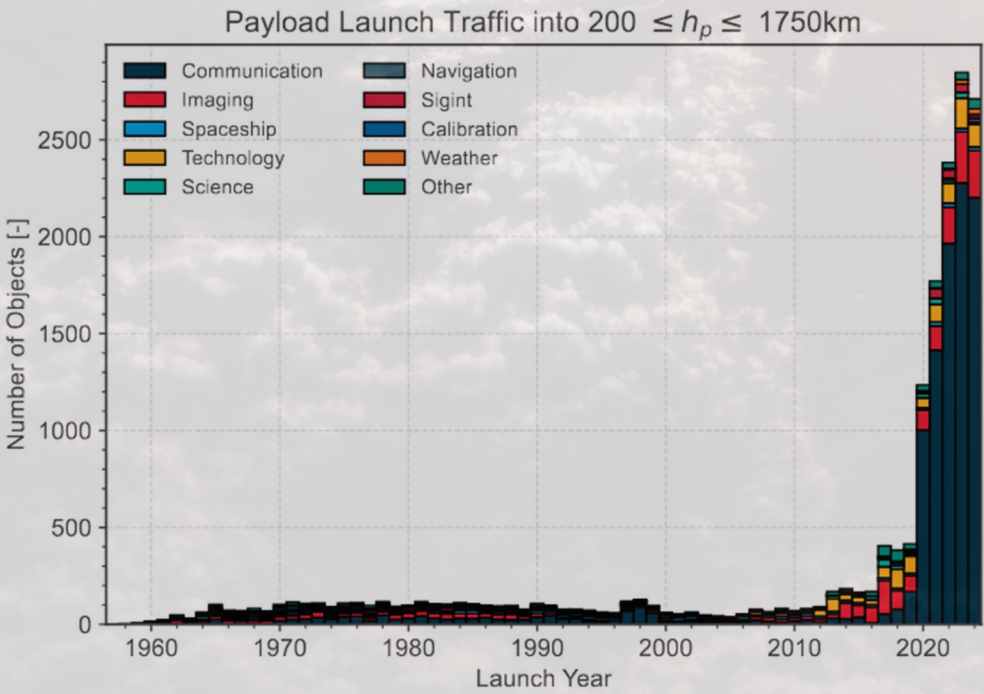
Any developer can be a space developer with the new Azure Orbital Space SDK >

Today, we are announcing a crucial step towards democratizing access to space development, with the private preview release of Azure Orbital Space Software Development Kit(SDK)—a secure hosting platform and application kit designed to enable developers to create in the cloud and deploy and operate applications



Note: AWS = Amazon Web Services, Inc.
Source: AWS. "AWS Ground Station."
<https://aws.amazon.com/ground-station/>,
accessed July 2025.

Source: Azure Microsoft. "Azure Orbital Ground Station."
<https://azure.microsoft.com/en-us/blog/content-type/announcements/>,
accessed July 2025.



Evolution of the launch traffic near LEO_{IADC} per mission type in object number (left) and mass (right).

Source: The European Space Agency/ESA Space Environment Report 2025."
https://www.esa.int/Space_Safety/Space_Debris/ESA_Space_Environment_Report_2025,
January 2025.



NAVIGATING CYBERSPACE CH

Cyberspace Targeting Methodology

Motivation

Intention

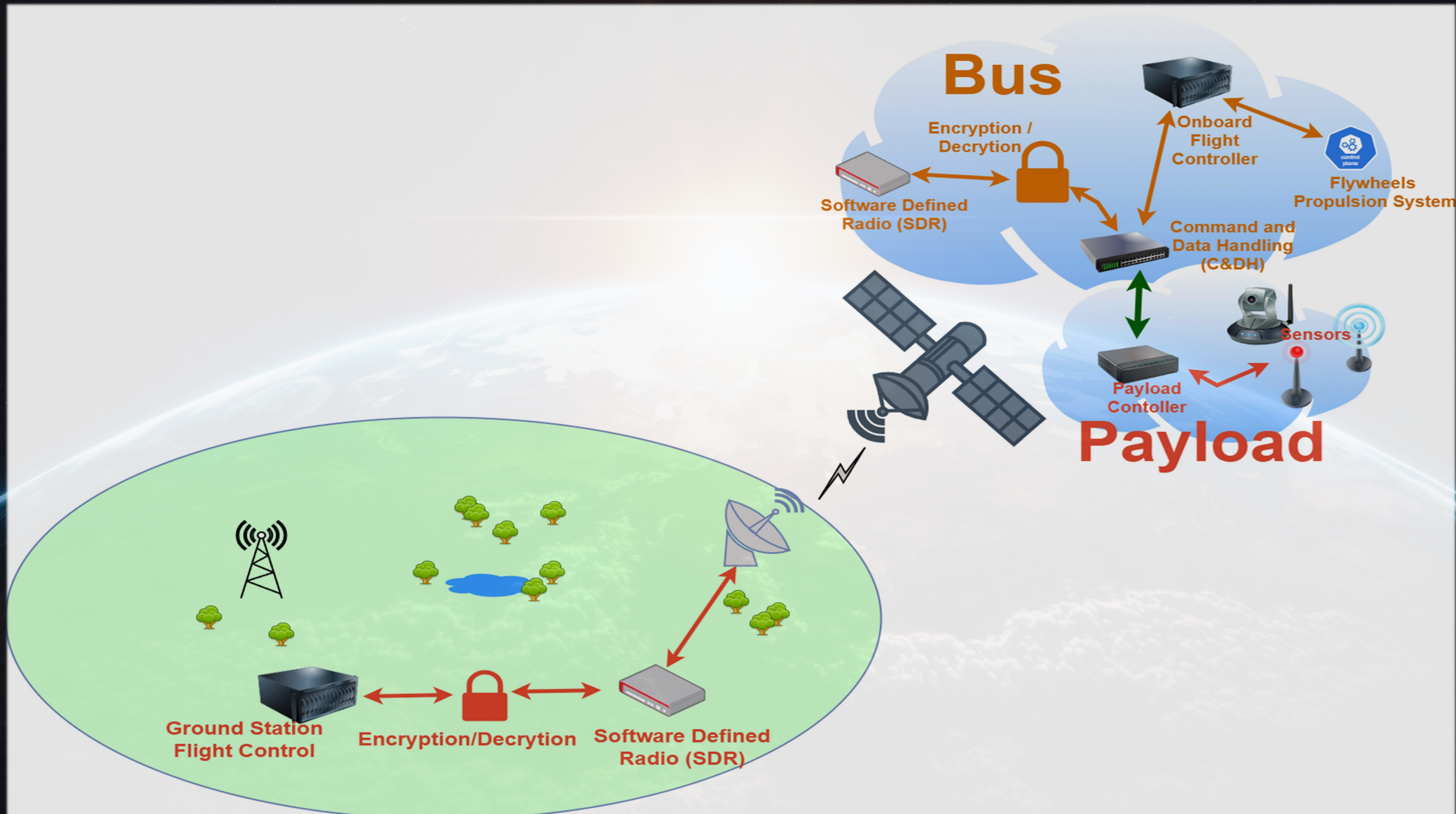
Opportunity

Confidentiality

Integrity

Availability







MITIGATIONS AND CONTR

Most modern satellite systems are engineered with multiple layers of safeguards and control mechanisms, emphasizing fault tolerance through hardware and software redundancy, along with embedded resilience features within their system architecture.

- **Deployment of secure gateways**
- **Use of field-programmable gate arrays**
- **Watchdog scripts or timers**
- **Gold image**
- **Secure boot and firmware verification**
- **Role-based access control**
- **Multifactor authentication**
- **Ground segment security**
- **Command authentication codes: A cryptographic hash to verify integrity**
- **End-to-end encryption: Advanced Encryption Standard 256 - Early stages exploring postquantum cryptography**
- **National Institute of Standards and Technology (NIST) Special Publications 800-53 and 800-171 and NIST Interagency Report 8270**

Space Attack Research & Tactic Analysis (SPARTA)

[show sub-techniques](#)[hide sub-techniques](#)

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Defense Evasion	Lateral Movement	Exfiltration	Impact
9 techniques	5 techniques	12 techniques	18 techniques	5 techniques	11 techniques	7 techniques	10 techniques	6 techniques
Gather Spacecraft Design Information ⁽⁹⁾	Acquire Infrastructure ⁽⁴⁾	Compromise Supply Chain ⁽³⁾	Replay ⁽²⁾	Memory Compromise ⁽⁰⁾	Disable Fault Management ⁽⁰⁾	Hosted Payload ⁽⁰⁾	Replay ⁽⁰⁾	Deception (or Misdirection) ⁽⁰⁾
Gather Spacecraft Descriptors ⁽³⁾	Compromise Infrastructure ⁽³⁾	Compromise Software Defined Radio ⁽⁰⁾	Position, Navigation, and Timing (PNT) Geofencing ⁽⁰⁾	Backdoor ⁽²⁾	Disrupt or Deceive Downlink ⁽³⁾	Exploit Lack of Bus Segregation ⁽⁰⁾	Side-Channel Exfiltration ⁽⁵⁾	Disruption ⁽⁰⁾
Gather Spacecraft Communications Information ⁽⁴⁾	Obtain Cyber Capabilities ⁽²⁾	Crosslink via Compromised Neighbor ⁽⁰⁾	Modify Authentication Process ⁽⁰⁾	Ground System Presence ⁽⁰⁾	On-Board Values Obfuscation ⁽¹²⁾	Constellation Hopping via Crosslink ⁽⁰⁾	Signal Interception ⁽²⁾	Denial ⁽⁰⁾
Gather Launch Information ⁽¹⁾	Stage Capabilities ⁽²⁾	Secondary/Backup Communication Channel ⁽²⁾	Compromise Boot Memory ⁽⁰⁾	Replace Cryptographic Keys ⁽⁰⁾	Masquerading ⁽⁰⁾	Visiting Vehicle Interface(s) ⁽⁰⁾	Out-of-Band Communications Link ⁽⁰⁾	Degradation ⁽⁰⁾
Eavesdropping ⁽⁴⁾	Obtain Non-Cyber Capabilities ⁽⁴⁾	Rendezvous & Proximity Operations ⁽³⁾	Exploit Hardware/Firmware Corruption ⁽²⁾	Credentialed Persistence ⁽⁰⁾	Subvert Protections via Safe-Mode ⁽⁰⁾	Virtualization Escape ⁽⁰⁾	Proximity Operations ⁽⁰⁾	Destruction ⁽⁰⁾
Gather FSW Development Information ⁽²⁾		Compromise Hosted Payload ⁽⁰⁾	Disable/Bypass Encryption ⁽⁰⁾		Modify Whitelist ⁽⁰⁾	Launch Vehicle Interface ⁽¹⁾	Modify Communications Configuration ⁽²⁾	Theft ⁽⁰⁾
Monitor for Safe-Mode Indicators ⁽⁰⁾		Compromise Ground System ⁽²⁾	Trigger Single Event Upset ⁽⁰⁾		Evasion via Rootkit ⁽⁰⁾	Credentialed Traversal ⁽⁰⁾	Compromised Ground System ⁽⁰⁾	
Gather Supply Chain Information ⁽⁴⁾		Rogue External Entity ⁽³⁾	Time Synchronized Execution ⁽²⁾		Evasion via Bootkit ⁽⁰⁾		Compromised Developer Site ⁽⁰⁾	
Gather Mission Information ⁽⁰⁾		Trusted Relationship ⁽³⁾	Exploit Code Flaws ⁽³⁾		Camouflage, Concealment, and Decoys (CCD) ⁽⁵⁾		Compromised Partner Site ⁽⁰⁾	
		Unauthorized Access During Safe-Mode ⁽⁰⁾	Malicious Code ⁽⁴⁾		Overflow Audit Log ⁽⁰⁾		Payload Communication Channel ⁽⁰⁾	
		Auxiliary Device Compromise ⁽⁰⁾	Exploit Reduced Protections During Safe-Mode ⁽⁰⁾		Credentialed Evasion ⁽⁰⁾			
		Assembly, Test, and Launch Operation Compromise ⁽⁰⁾	Modify On-Board Values ⁽¹³⁾					
			Flooding ⁽²⁾					
			Spoofing ⁽⁵⁾					
			Side-Channel Attack ⁽⁰⁾					
			Jamming ⁽³⁾					
			Kinetic Physical Attack ⁽²⁾					
			Non-Kinetic Physical Attack ⁽³⁾					

Considered the MITRE Adversarial Tactics, Techniques, and Common Knowledge Framework for space attacks, SPARTA is intended to provide unclassified information to space professionals about how spacecraft may be compromised, sharing tactics, techniques, and procedures.

MALWARE AND ADVANCE THREAT ACTORS

Serpent Chaser

The 2020 “**Serpent Chaser**” attack targeted a European aerospace company, aiming to steal sensitive satellite technology and highlighted the ongoing and evolving threats faced by satellite systems in the contemporary cybersecurity landscape.

Attribution: Unofficially linked to Russian APT28

Mitigation: Secure firmware pipeline

Method: Spear phishing, zero-day exploitation

Malware 4.STL

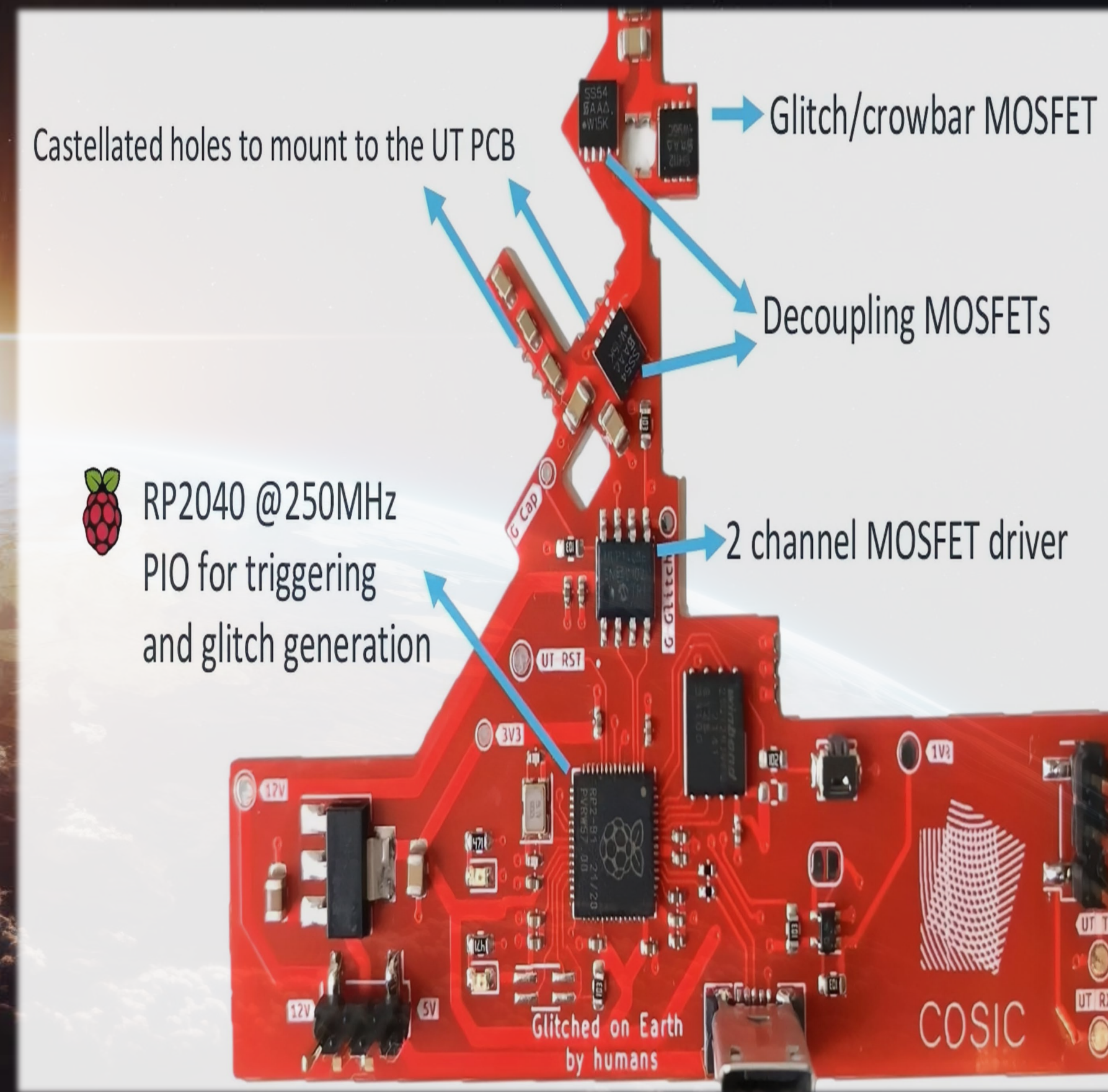
More recently (2024), **Malware 4.STL** operates by leveraging compromised mobile devices, particularly Android tablets used by Ukrainian military personnel, to gather sensitive data about Starlink satellite terminals. The malware collects data available via application programming interface functions on the mobile device, including information about the configuration of connected Starlink satellite terminals.

Attribution: Linked to Russian Sandworm APT44

Mitigation: Endpoint detection and response, software updates, device management

Method: Spread the malware using captured Ukrainian tablets on the battlefield


```
288 Development login enabled: yes
289
290
291 SpaceX User Terminal.
292
293 user1 login: root
294 Password:
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312 The Flight Software does not log to the console. If you wish to view
313 the output of the binaries, you can use:
314
315 tail -f /var/log/messages
316
317 Or view the viceroy telemetry stream.
318
319 <0x1b>7<0x1b>[r<0x1b>[999;999H<0x1b>[6n[root@user1 ~]# id
320 uid=0(root) gid=0(root) groups=0(root),10(wheel),1000(signers)
```



Note: MOSFET = metal-oxide-semiconductor field-effect transistor, UT = ultrasonic testing, PCB = printed circuit board, PIO = programmable input/output.

Source: Wouters, L. "Glitched on Earth by Humans: A BlackBox Security Evaluation of the SpaceX Starlink User Terminal." Black Hat USA 2022, <https://i.blackhat.com/USA22/Wednesday/US22-Wouters-Glitched-On-Earth.pdf>, 2022.



POC 1

Digital-Twin Sandbox

Designed for comprehensive integration and collaborative
over space mission simulations.

FileHelp

Computer Clock

ComputerStatusMessage
Ticks [ns] 6169999990
State Running
ID 3dc8e9c5-47d0-4e46-be27-42e51ca38e7b

Spacecraft Partitioned Data Storage

DataStorageMessage
Capacity [B] 10485760
Allocated [B] 0
Partitions 0
ID 0fe70960-8e61-416f-b332-2982a8ed65ed

Perth -> Spacecraft Link Budget

DataLinkMessage
Connected False
Type Radio
Frequency [Hz] 900021005.828018
Bandwidth [Hz] 10000000
ConnectionFraction 0
Distance [m] 1996792.73601696
DeltaVelocity [m/s] 6997.09868189646
SignalToNoise [dB] 0
TransmissionRate [bps] 0
Passes 0
CurrentPassTime [s] 0
TotalPassTime [s] 0
CurrentData [Mb] 0
TotalData [Mb] 0
ID 41c07623-826a-414c-bb7f-62fae397

Spacecraft -> Brisbane Link Budget

DataLinkMessage
Connected False
Type Radio
Frequency [Hz] 5400114633.76203
Bandwidth [Hz] 10000000
ConnectionFraction 0
Distance [m] 5492594.461294
DeltaVelocity [m/s] 6364.13657917641
SignalToNoise [dB] 0
TransmissionRate [bps] 0
Passes 0
CurrentPassTime [s] 0
TotalPassTime [s] 0
CurrentData [Mb] 0
TotalData [Mb] 0
ID 3f57e7e4-6048-4221-a74f-e31d2656

Next Command

Options

Location: 34.90 °S, 94.66 °E, 300.00 km
Local Time: 12:15:51
Computer State: Running
Guidance Pointing: Ground

Nominal Editor Preview [NetMode: Standalone 0] (64-bit/PC D3D SM6)

Nominal Editor - Demo_DataNetwork

EarthSpacecraftChassis 3U

60.8 s 50x 01/0

Bytes Transmitted on Network

Time (m.s) 00m12s 00m24s 00m36s 00m48s

Ground: Bytes Transmitted 0

Spacecraft: Bytes Transmitted 0

Data Storage

Time (m.s) 00m12s 00m24s 00m36s 00m48s

Ground: Allocated 0

Spacecraft: Allocated 0

Signal to Noise

Time (m.s) 00m12s 00m24s 00m36s 00m48s

Perth: Signal To Noise 0

Brisbane: Signal To Noise 0

Attitude Pointing Error

Time (m.s) 00m12s 00m24s 00m36s 00m48s

STAGE 1

The spacecraft is attempting to align with the Perth ground station.

This demo showcases the advanced TT&C system. A ground station (Perth) will uplink 5 commands to the spacecraft. The spacecraft will execute each command in order, including pointing and data recording. The state of the IMU will be tracked internally and then downlinked to the second ground station (Brisbane) on the last command. Finally, this data is exported to a CSV file. All communication is done using the simulated network with packets and byte array communication. On-board data storage modules are on both the spacecraft and final ground station.

Options

AllSelectedConstellation

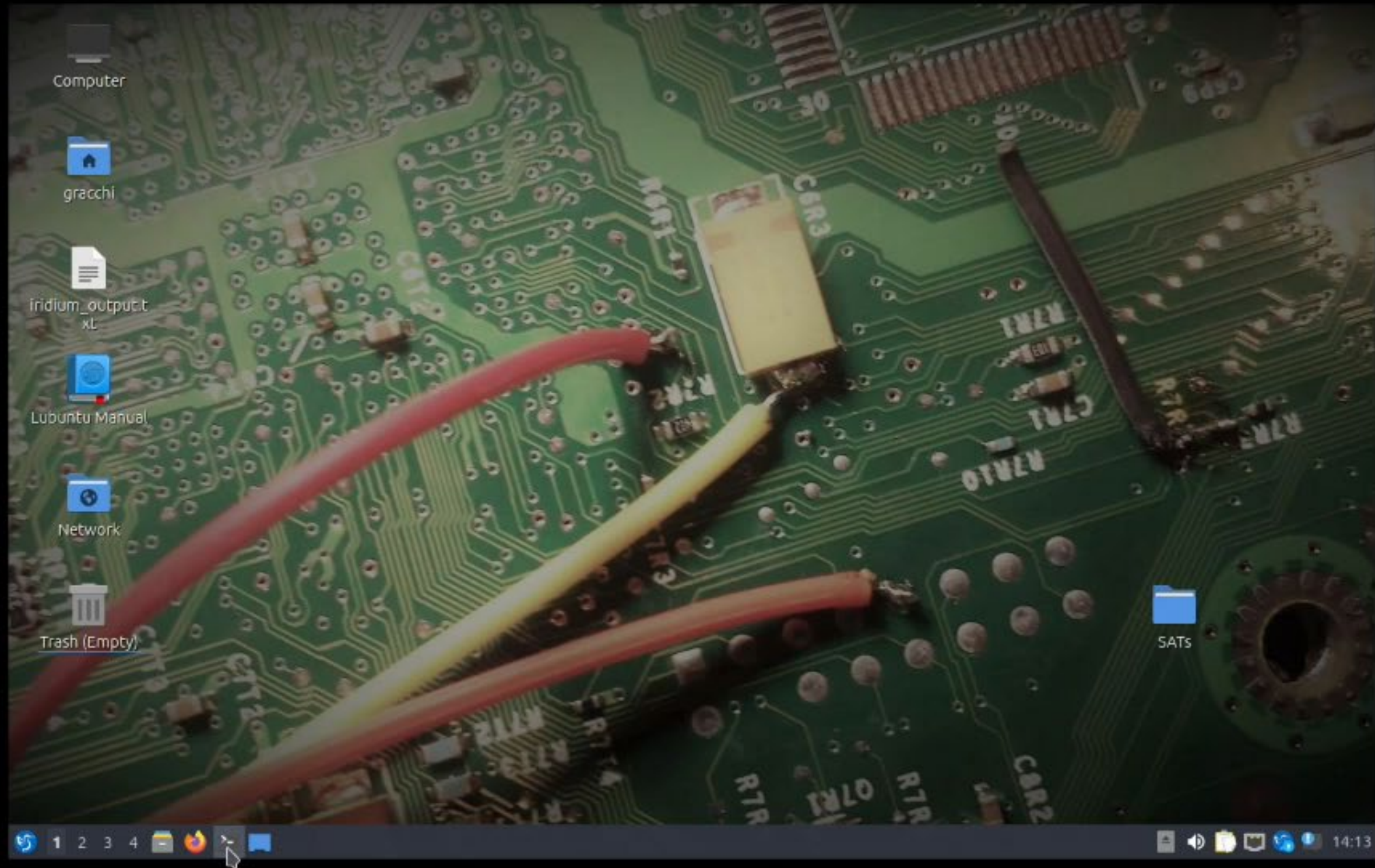
World map showing Perth, Brisbane, and Spacecraft location.



POC 2

Satellite Interception

Disclaimer: This video is intended for educational and research purposes only.





THANK YOU

CHADI SALIBY