CSIAC

CYBERSPACE SECURITY

LOW EARTH ORBIT

CHADI SALIBY

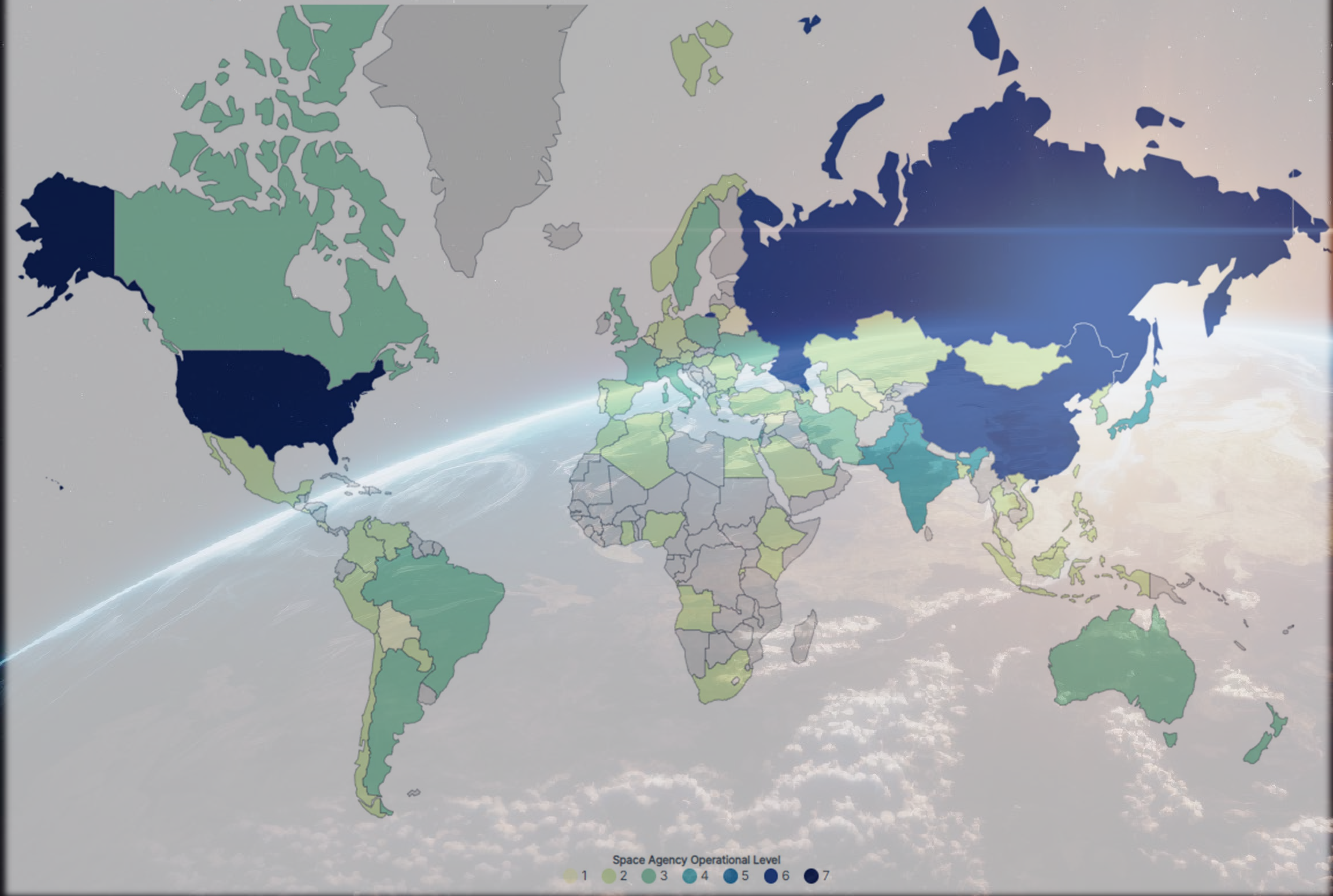
Background Image Source: https://www.freepik.com/premium -photo/nightly -earth-planet-outer-space-with-sun-flare_40045770.htm

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 Date." worldpopulationreview.com, accessed July 2250

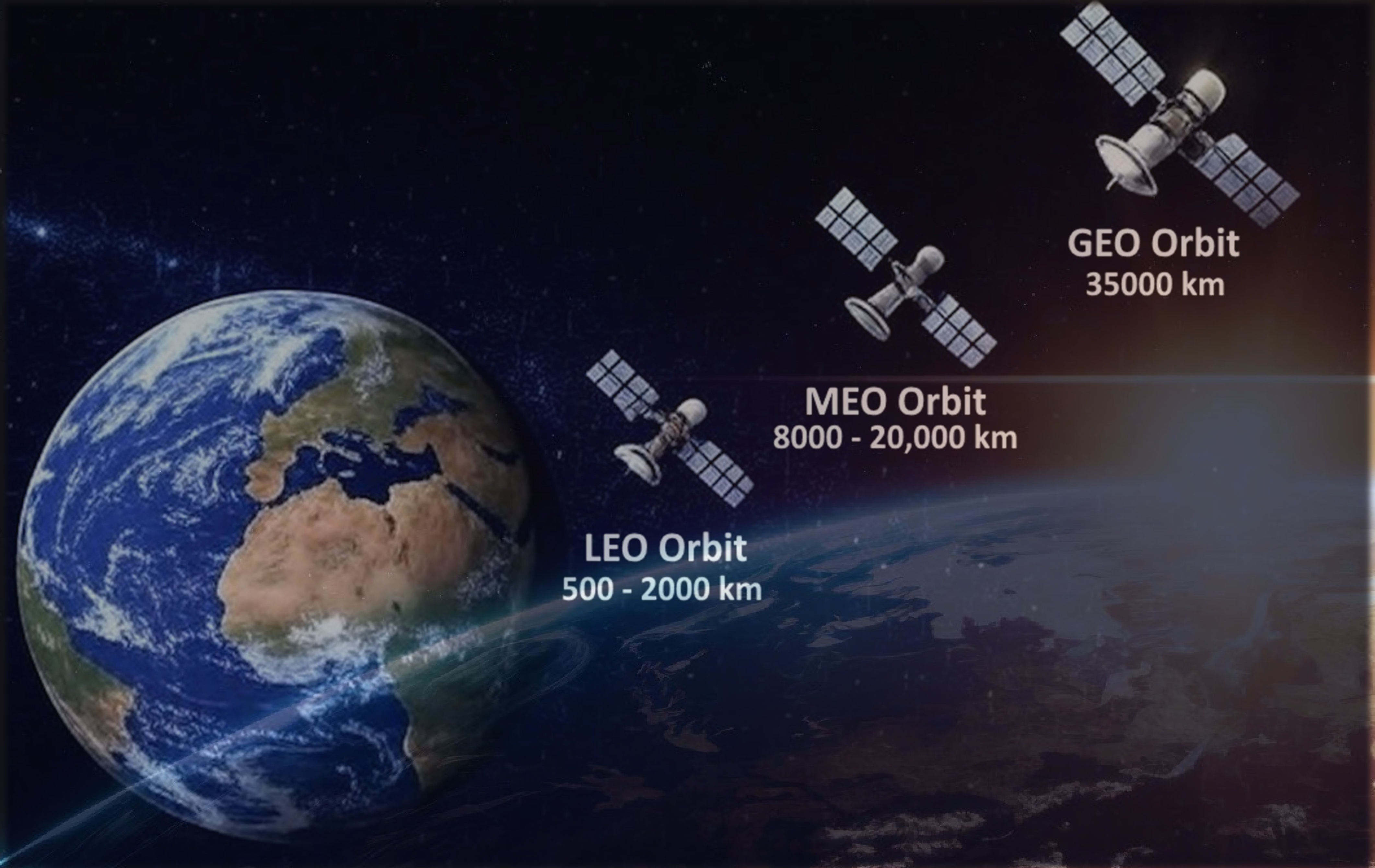
1U Standard Dimensions: 10 cm × 10 cm × 11 cm

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

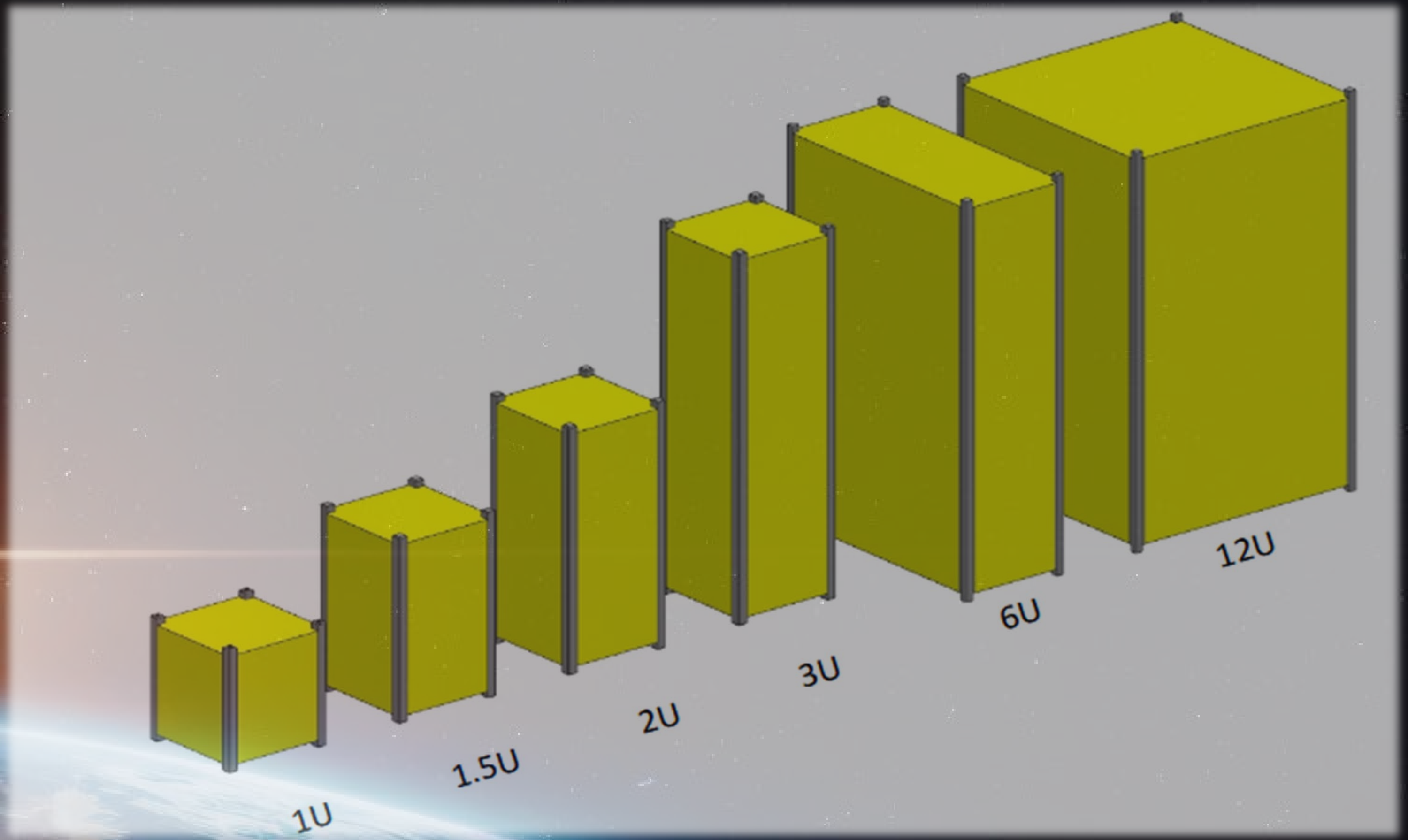
FIGURE 2: 1U CubeSat CP1 (left) 3U CubeSat CP10 (right) [Cal Poly]

Source: National Aeronautics and Space Administration (NASA). "CubeSat 101." https://www.nasa.gov/wp-content/uploads/2017/03/nasa_csli_cubesat_101_508.pdf, October 2017.

IT'S ALL IN THE ATTITUD

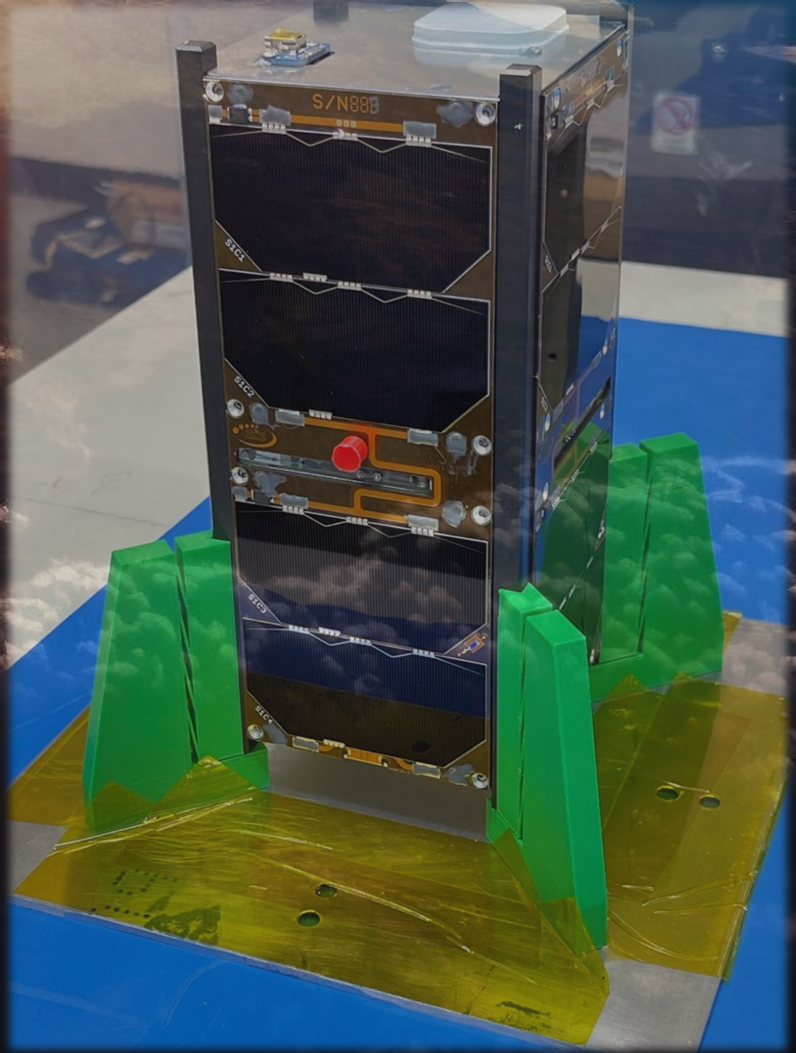


Note: GEO = geospatial earth orbit, MEO = medium earth orbit.
Source: Saliby, C. Created using draw.io.



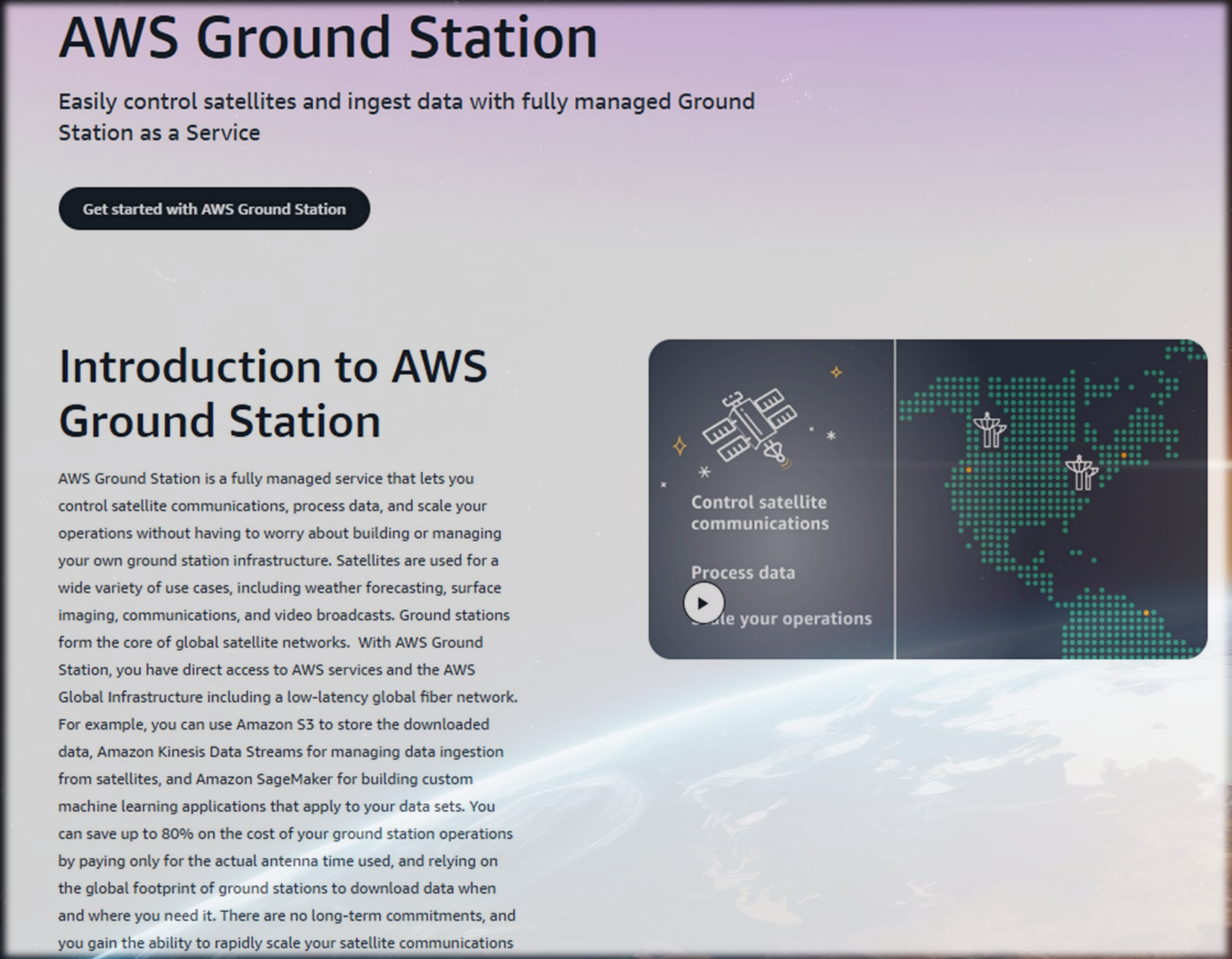
U Configuration	Mass [kg]
1U	2.00
1.5U	3.00
2U	4.00
3U	6.00
6U	12.00
12U	24.00

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



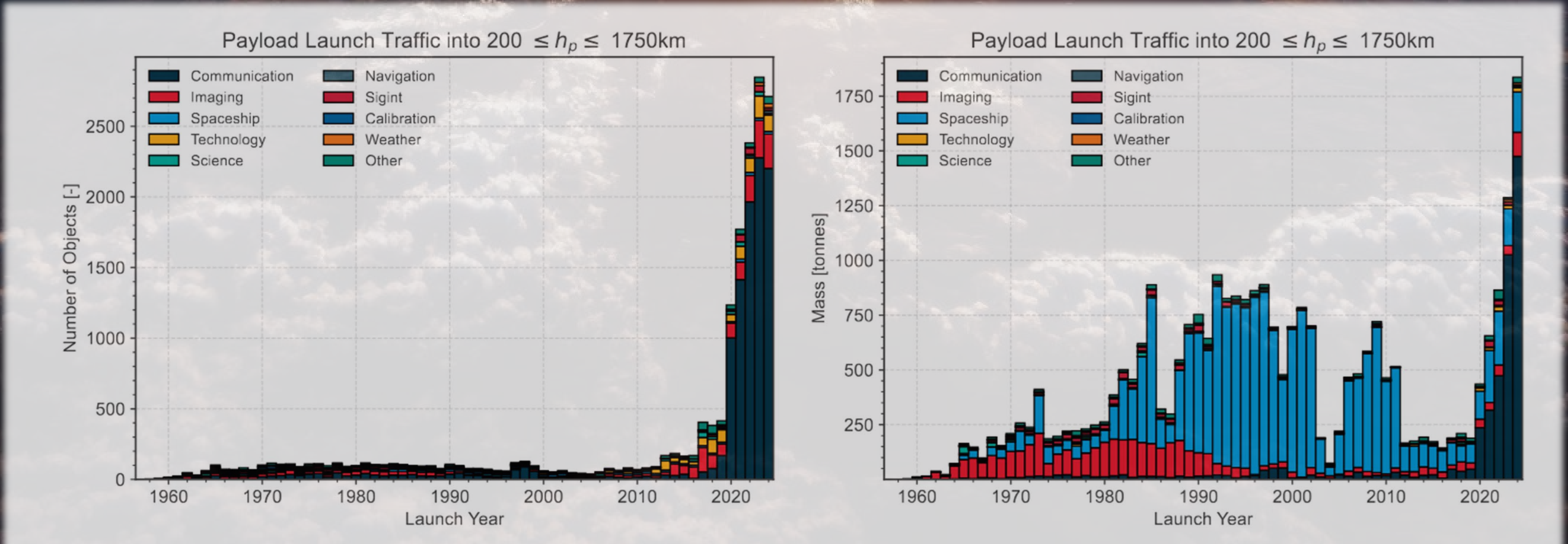
TJREVERB CubeSat, by Thomas Jefferson High School for Science and Technology
2U CubeSat (10 cm × 10 cm × 22.7 cm)

Source: NASA. "Astronomy Picture of the Day: Earth at Night." https://apod.nasa.gov/apod/ap001127.html, 27 November 2000.



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

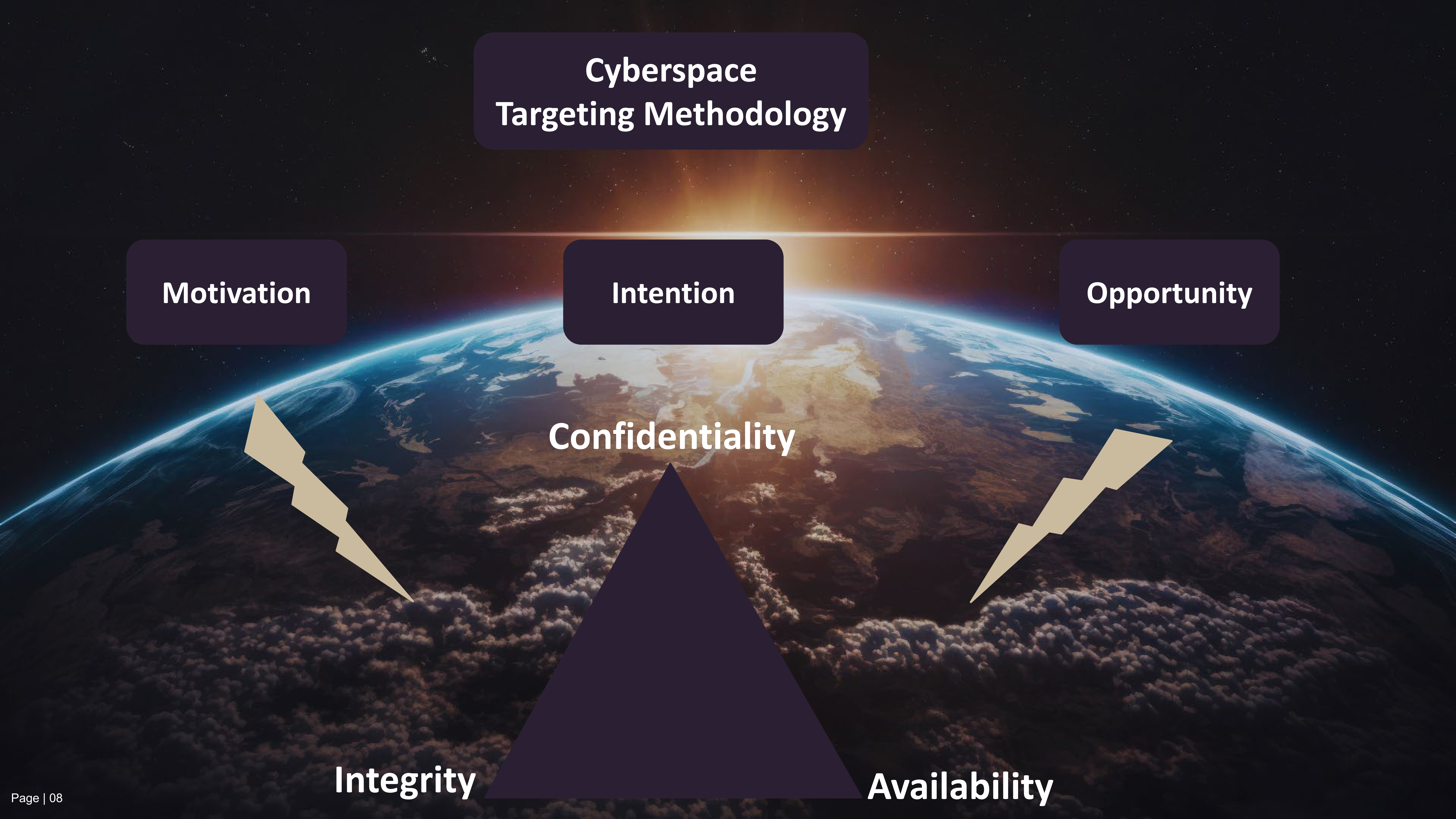
Source: Azure Microsoft. "Azure Orbital Ground Station." https://azure.microsoft.com/en-us/blog/content-type/announcements/, accessed July 2025.



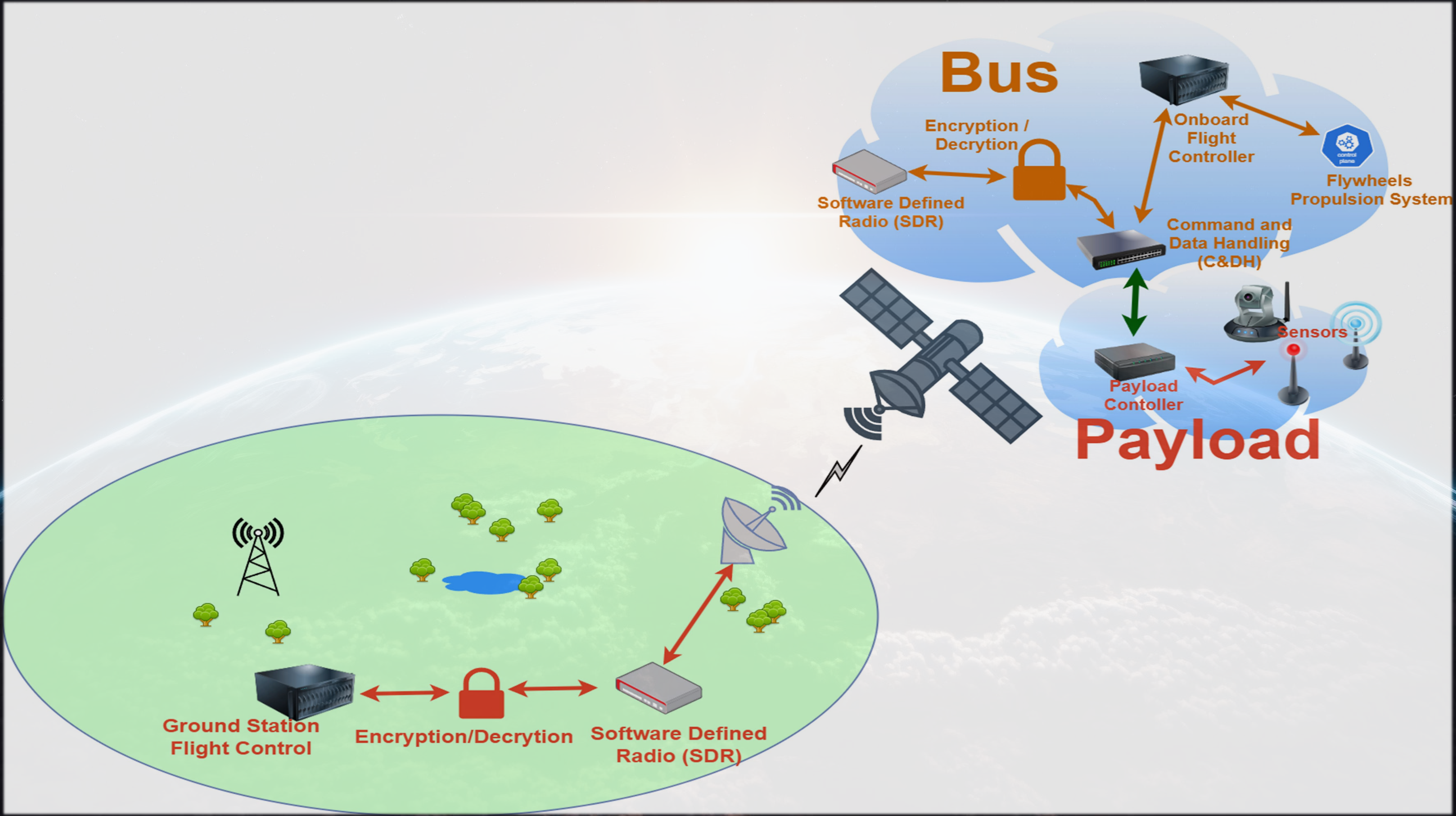
Evolution of the launch traffic near LEO_{IADC} per mission type in object number (left) and mass (right).

Source: The European Space Agency, "ESA Space Environment Report 2025." https://www.esa.int/Space_Safety/Space_Debris/ESA_Space_Environment_Report_2025, 4 January 2025.

NAVIGATING CYBERSPACE CH


Cyberspace
Targeting Methodology
Motivation
Intention
Opportunity
Confidentiality
Integrity
Availability

Source: https://www.istockphoto.com/en/video/satellite-receiving-signals-from-earth-gm948713036-259003768



Source: Created using draw.io – C.Saliby

Source: Pixabay. 2025. https://pixabay.com/videos/codingscreen-hacker-data-network-41263/

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 9 techniques	Resource Development 5 techniques	Initial Access 12 techniques	Execution 18 techniques	Persistence 5 techniques	Defense Evasion 11 techniques	Lateral Movement 7 techniques	Exfiltration 10 techniques	Impact 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

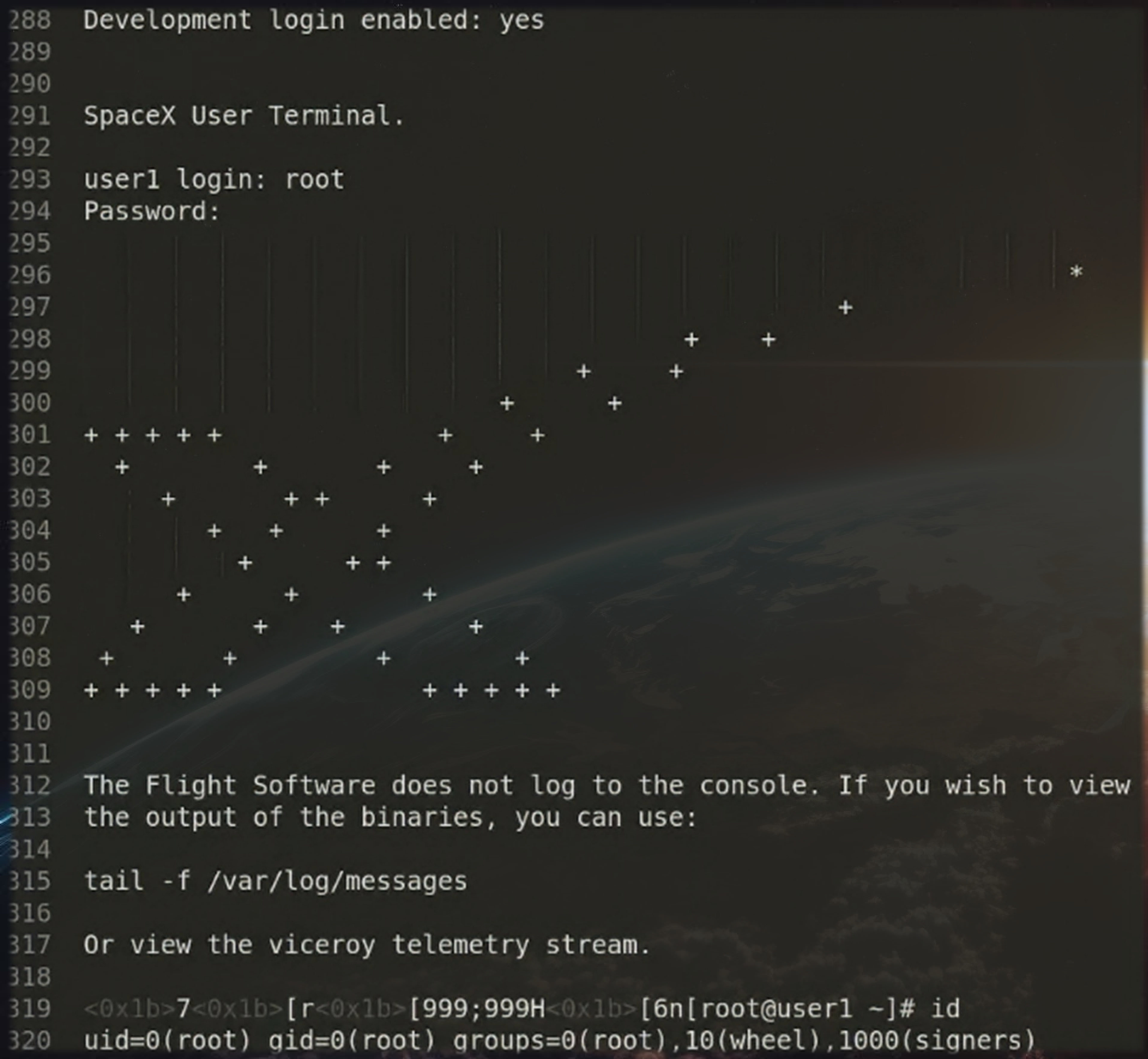
The 2020 "**Serpent Chaser**" attack targeted a European aerospace company, aiming to steal sensitive satellite technology and highlighted the ongoing and evolving threats faced by satellite systems in the contemporary cybersecurity landscape.

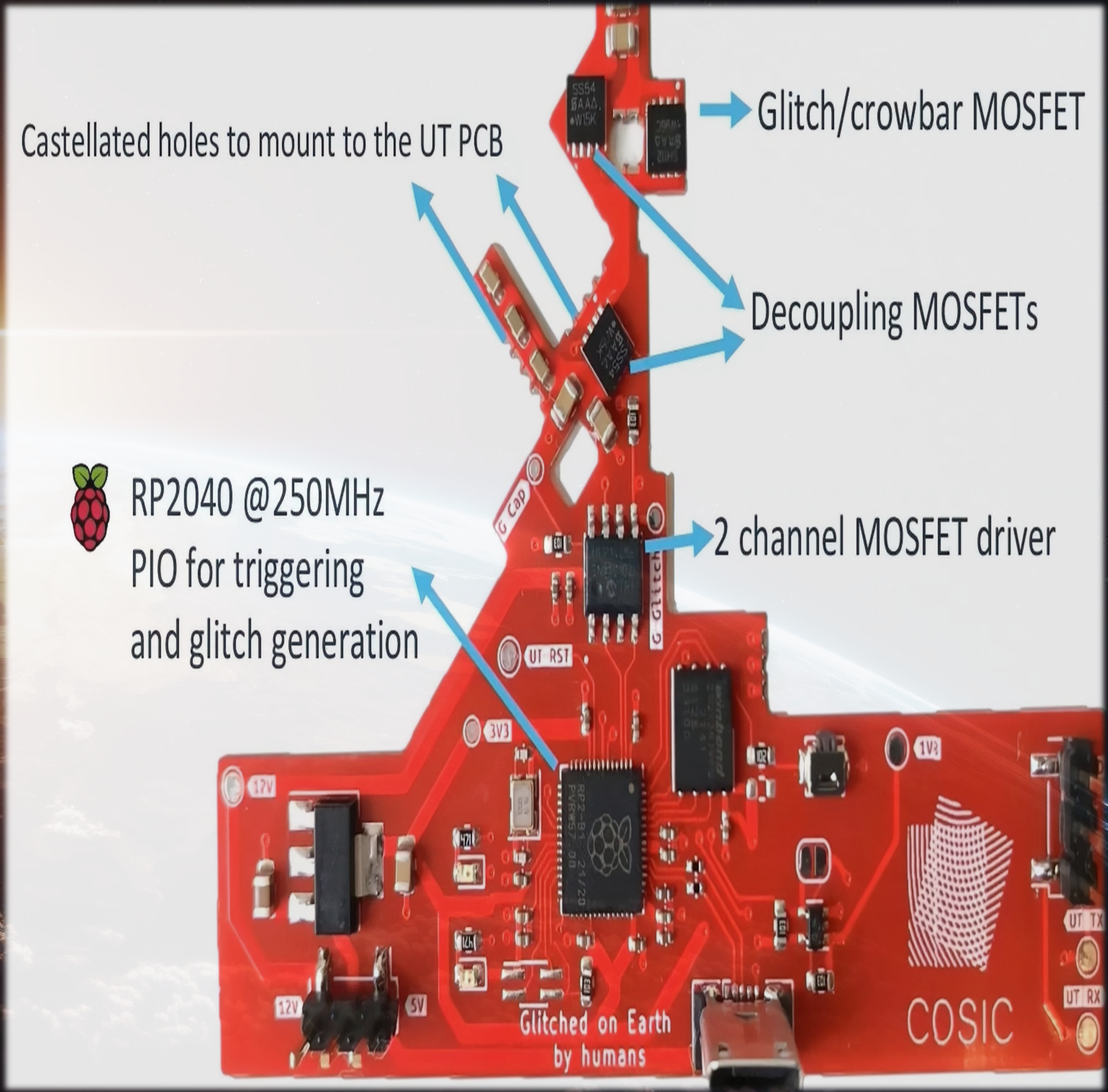
Attribution: Unofficially linked to Russian APT28
Mitigation: Secure firmware pipeline
Method: Spear phishing, zero-day exploitation

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 programing 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





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 Black-Box Security Evaluation of the SpaceX Starlink User Terminal." Black Hat USA 2022, https://i.blackhat.com/USA-22/Wednesday/US22-Wouters-Glitched-On-Earth.pdf, 2022.

POC 1

Digital-Twin Sandbox

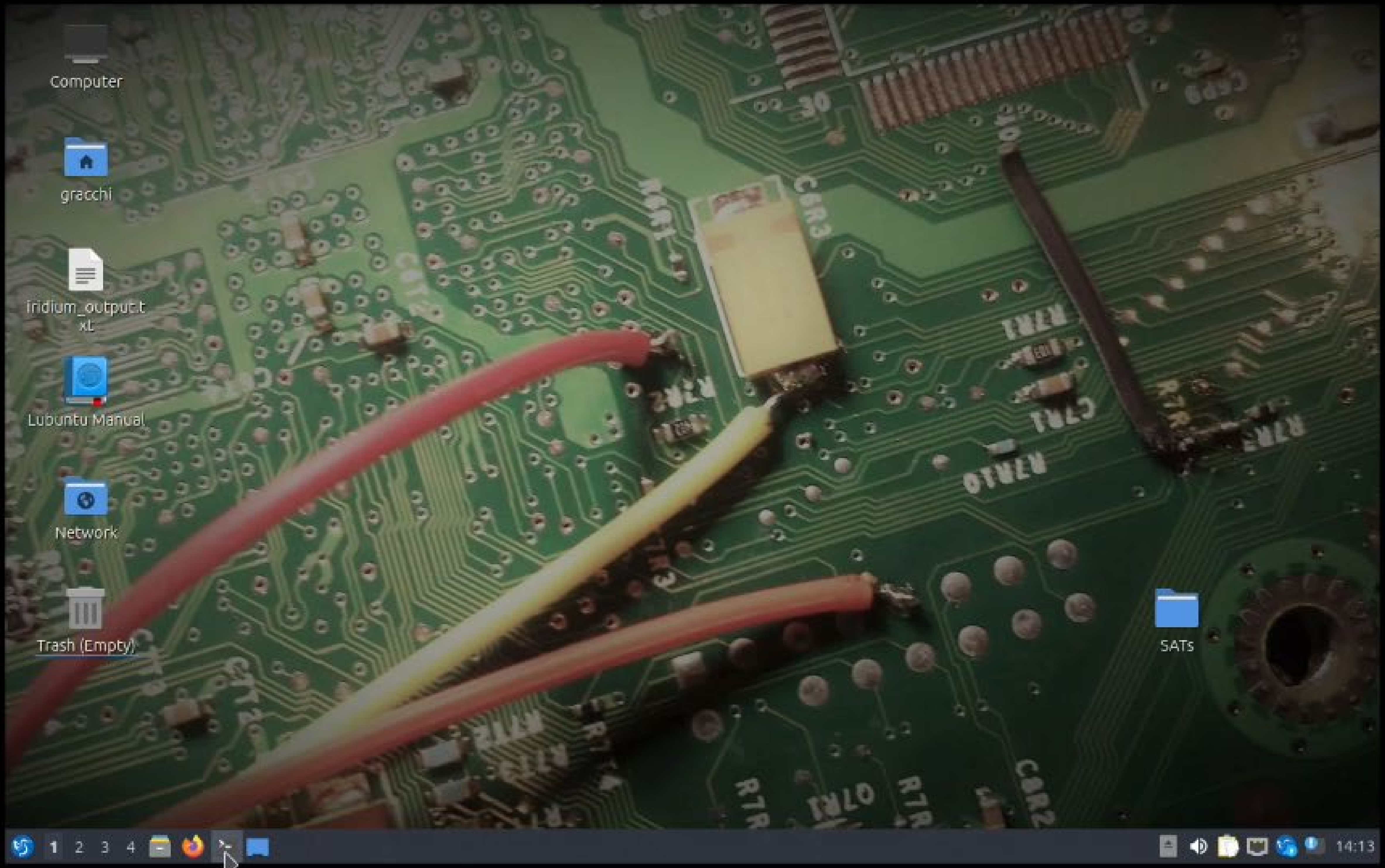
Designed for comprehensive integration and collaborative over space mission simulations.


Nominal Editor Preview [NetMode: Standalone 0] (64-bit/PC D3D SM6)
File Help
Nominal Editor - Demo_DataNetwork
60.8 s
50x
Computer Clock
ComputerStatusMessage
Ticks [ns] 61699999980
State Running
Spacecraft Partitioned Data Storage
DataStorageMessage
Capacity [B] 10485760
Allocated [B] 0
Partitions 0
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
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
Next Command
Console
Options
Earth
Spacecraft
Chassis 3U
Location: 34.90 °S, 94.66 °E, 300.00 km
Local Time: 12:15:51
Computer State: Running
Guidance Pointing: Ground
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
All
Selected
Constellation
Brisbane
Bytes Transmitted on Network
00m12s
00m24s
00m36s
Time (m:s)
Ground: Bytes Transmitted
Spacecraft: Bytes Transmitted
Data Storage
Ground: Allocated
Spacecraft: Allocated
Signal to Noise
Perth: Signal To Noise
Brisbane: Signal To Noise
Attitude Pointing Error

POC 2

Satellite Interception

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


Computer
gracchi
iridium_output.txt
Lubuntu Manual
Network
Trash (Empty)
SATs
1 2 3 4
14:13

THANK YOU

CHADI SALIBY