Orbital Security

Results of an Academic Work on New Space Satellite Security

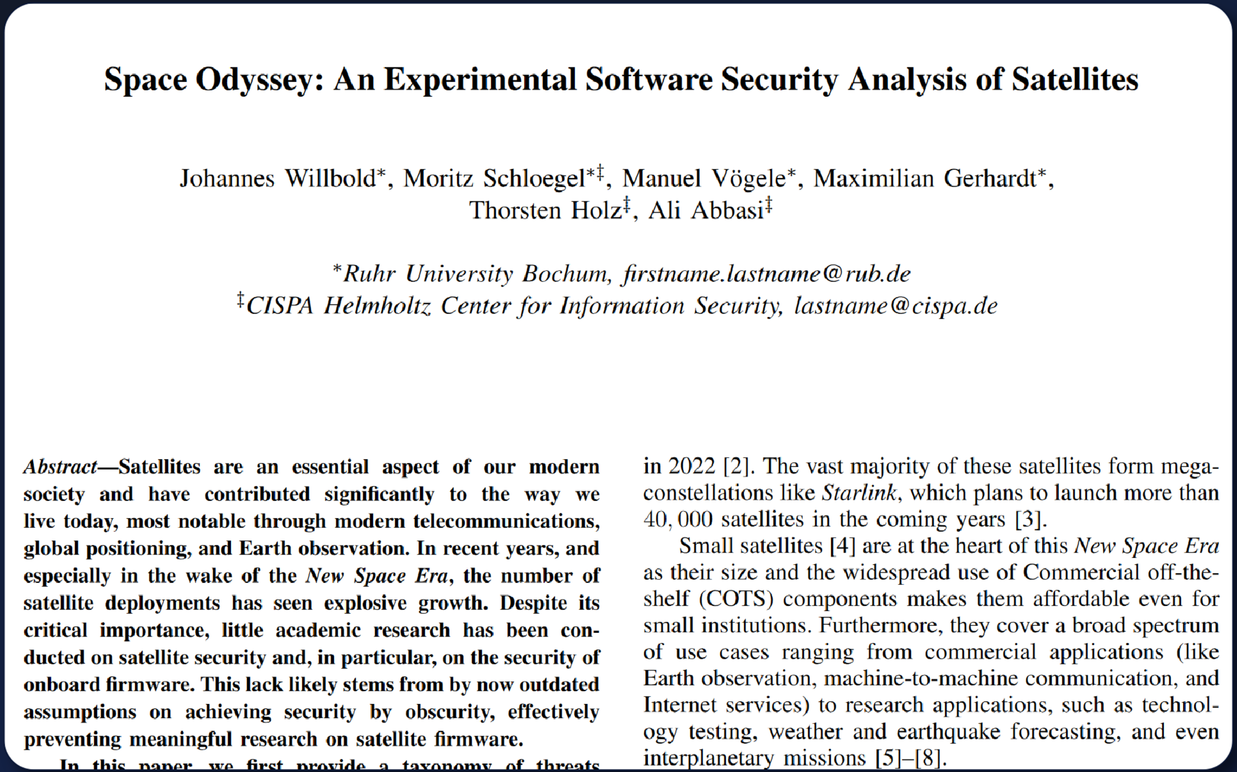
Johannes Willbold

in /jwillbold

$whoami

- Satellite & Space Systems Security
- Doctoral Student
  - Ruhr University Bochum, DE
- Visiting Researcher
  - Cyber-Defence Campus, CH
- General Chair @ SpaceSec
- IEEE S2CY Integration Layer Chair
- Hack-a-Sat 2 & 4 Finals

Space Odyssey



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 This lack likely stems from by now outdated assumptions on achieving security by obscurity, effectively preventing meaningful research on satellite firmware.**

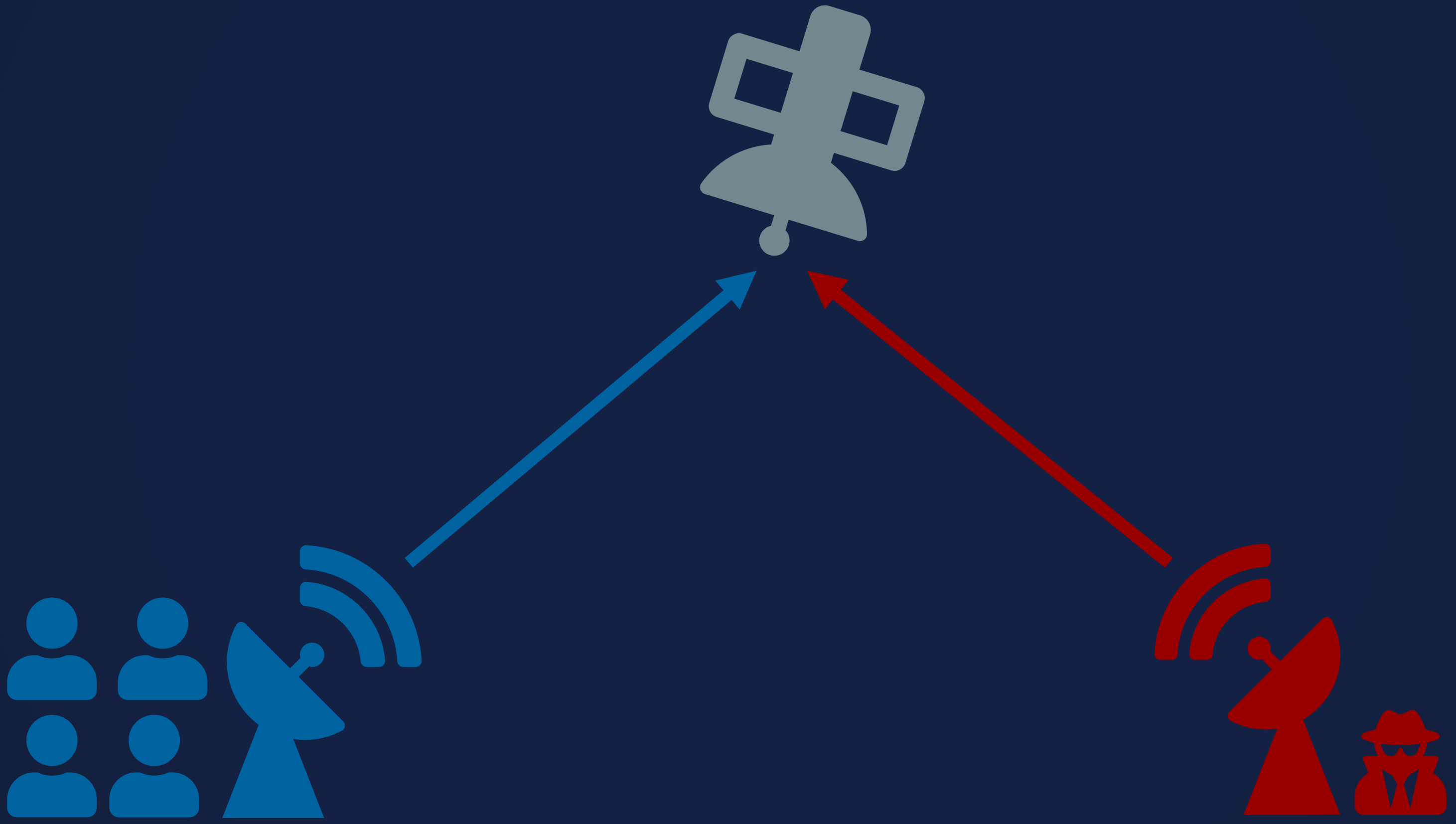
In this paper, we first provide a taxonomy of threats

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].

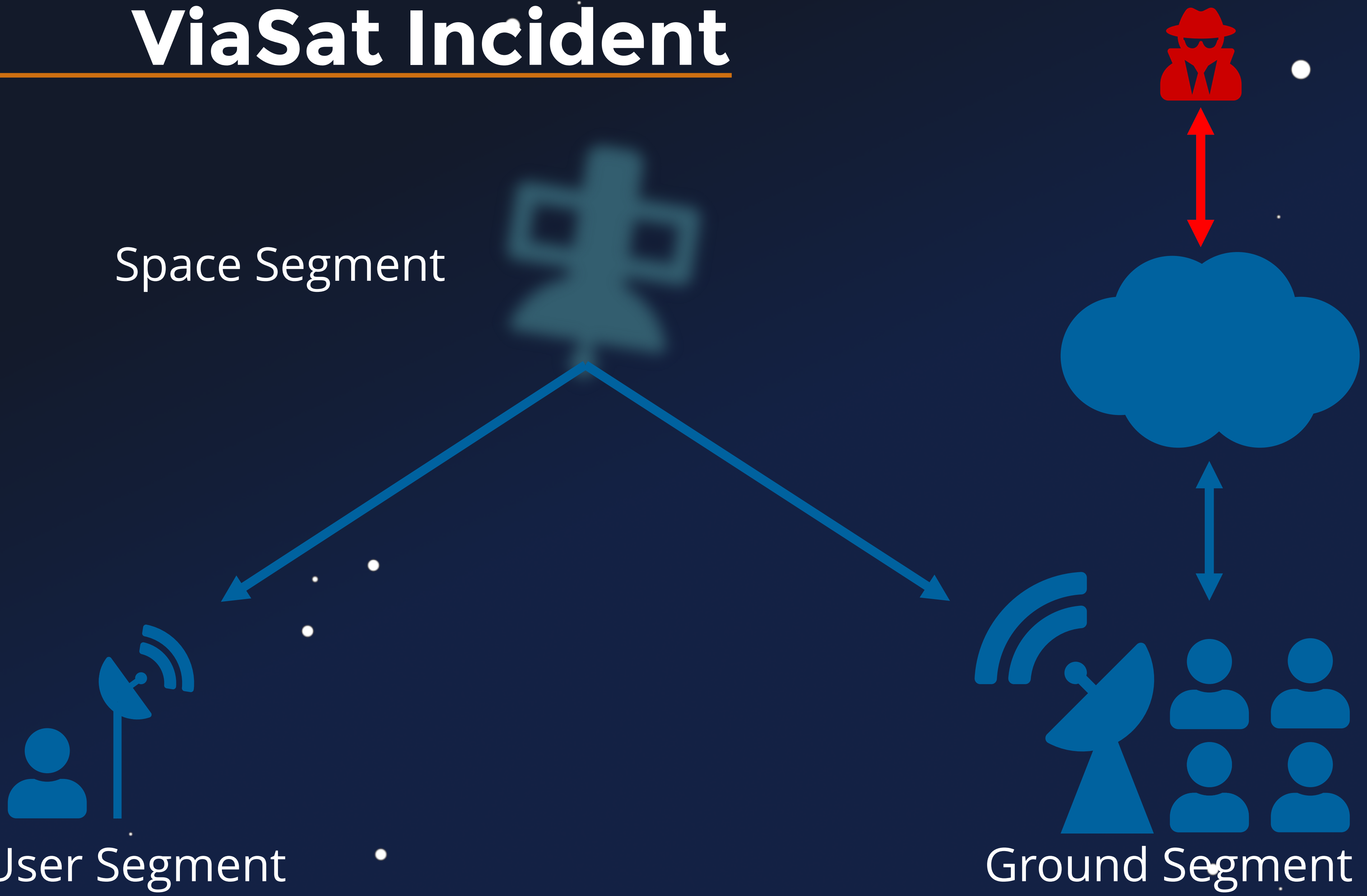
Small satellites [4] are at the heart of this *New Space Era* as their size and the widespread use of Commercial off-the-shelf (COTS) components makes them affordable even for small institutions. Furthermore, they cover a broad spectrum of use cases ranging from commercial applications (like Earth observation,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

44th IEEE Symposium on Security and Privacy (S&P)

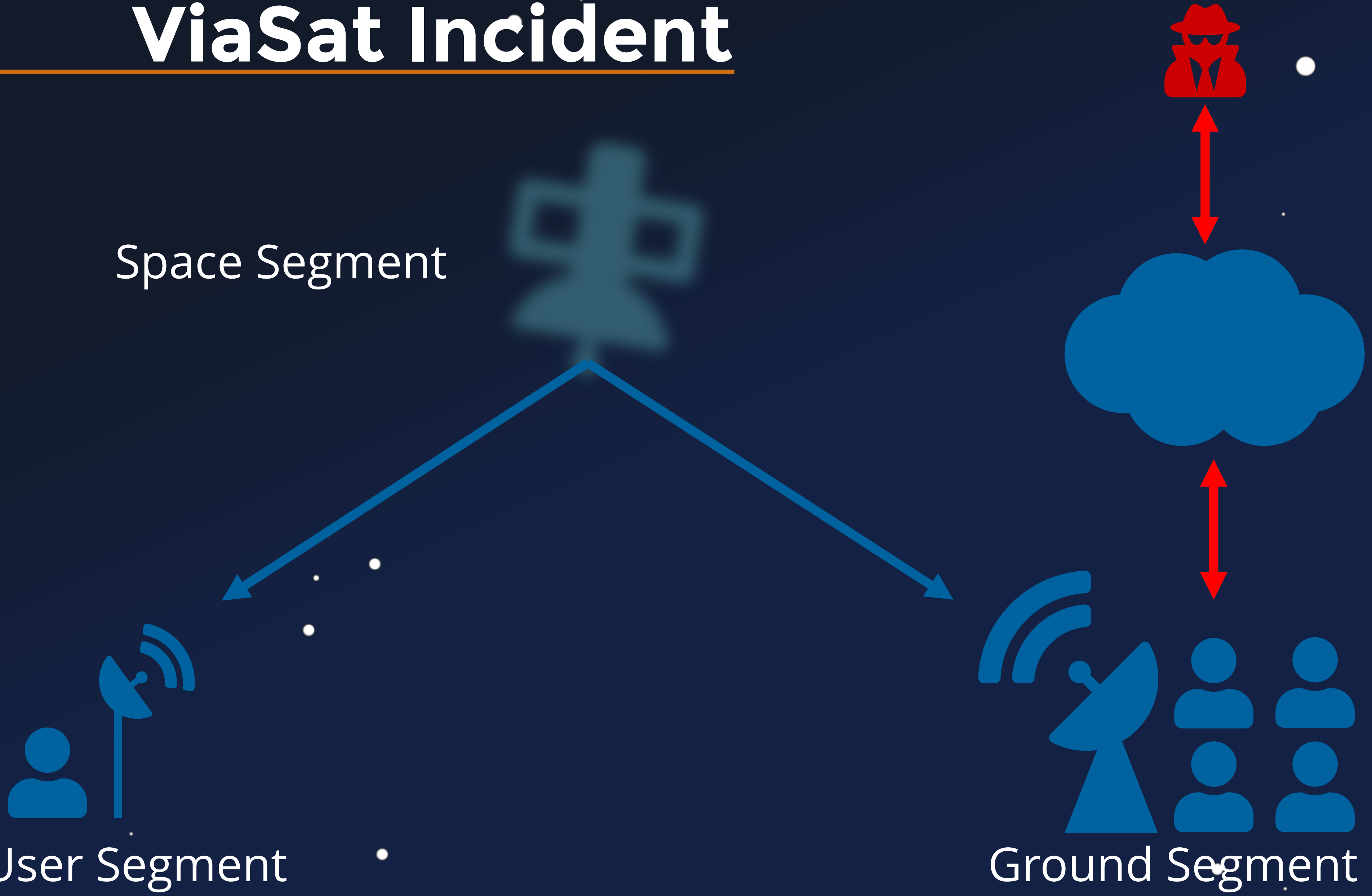
Firmware Attacks



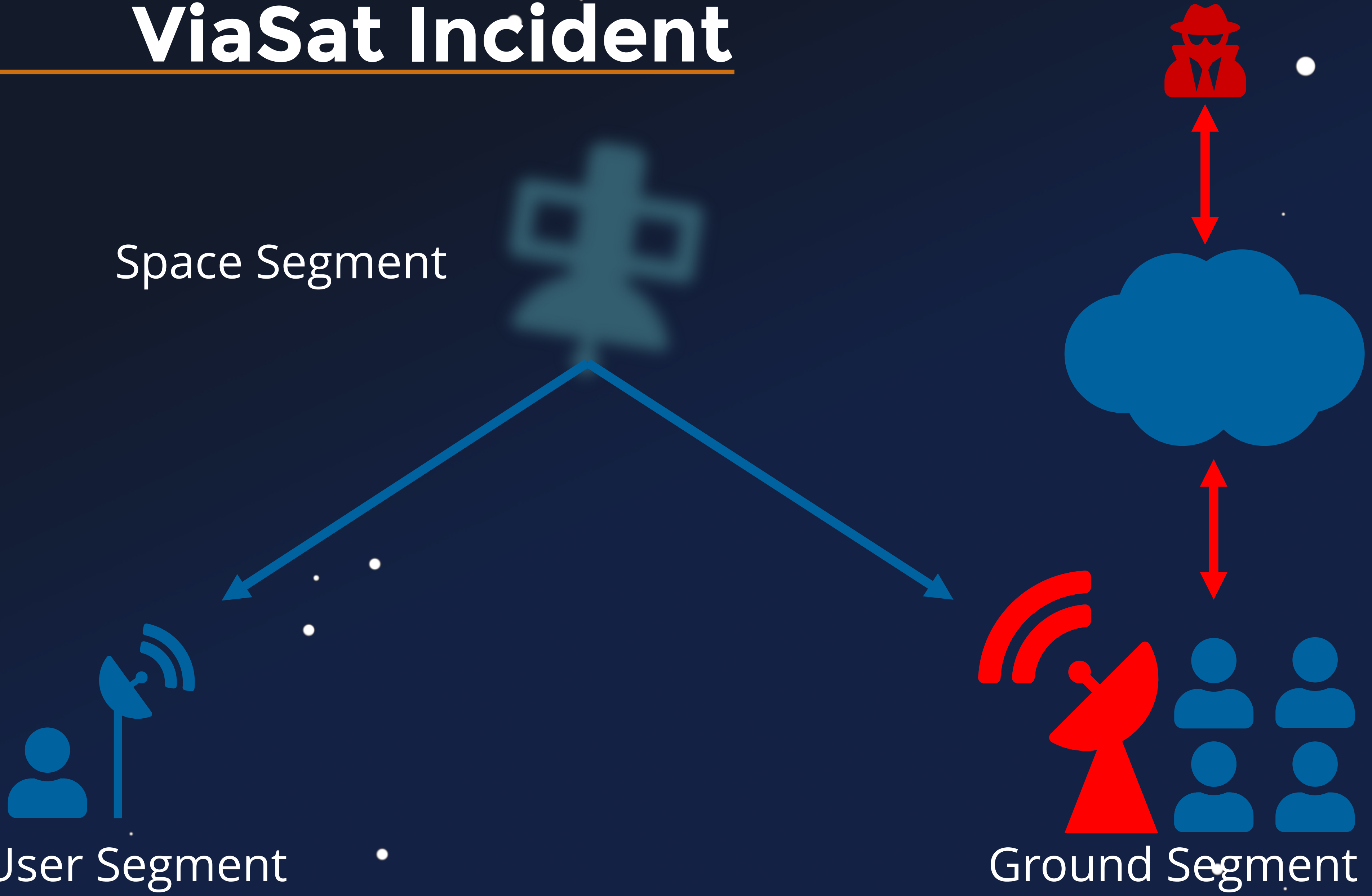
ViaSat Incident



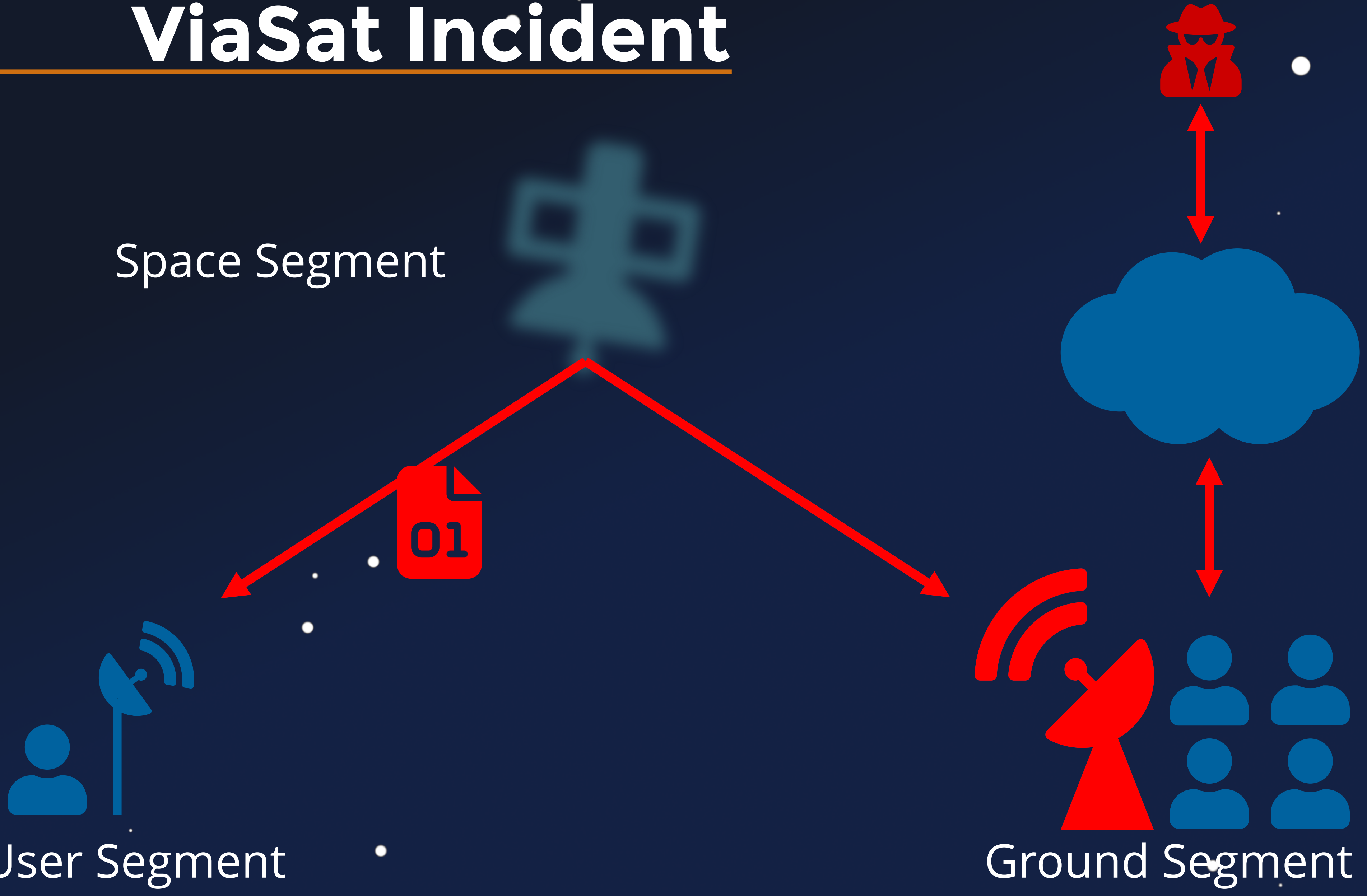
ViaSat Incident



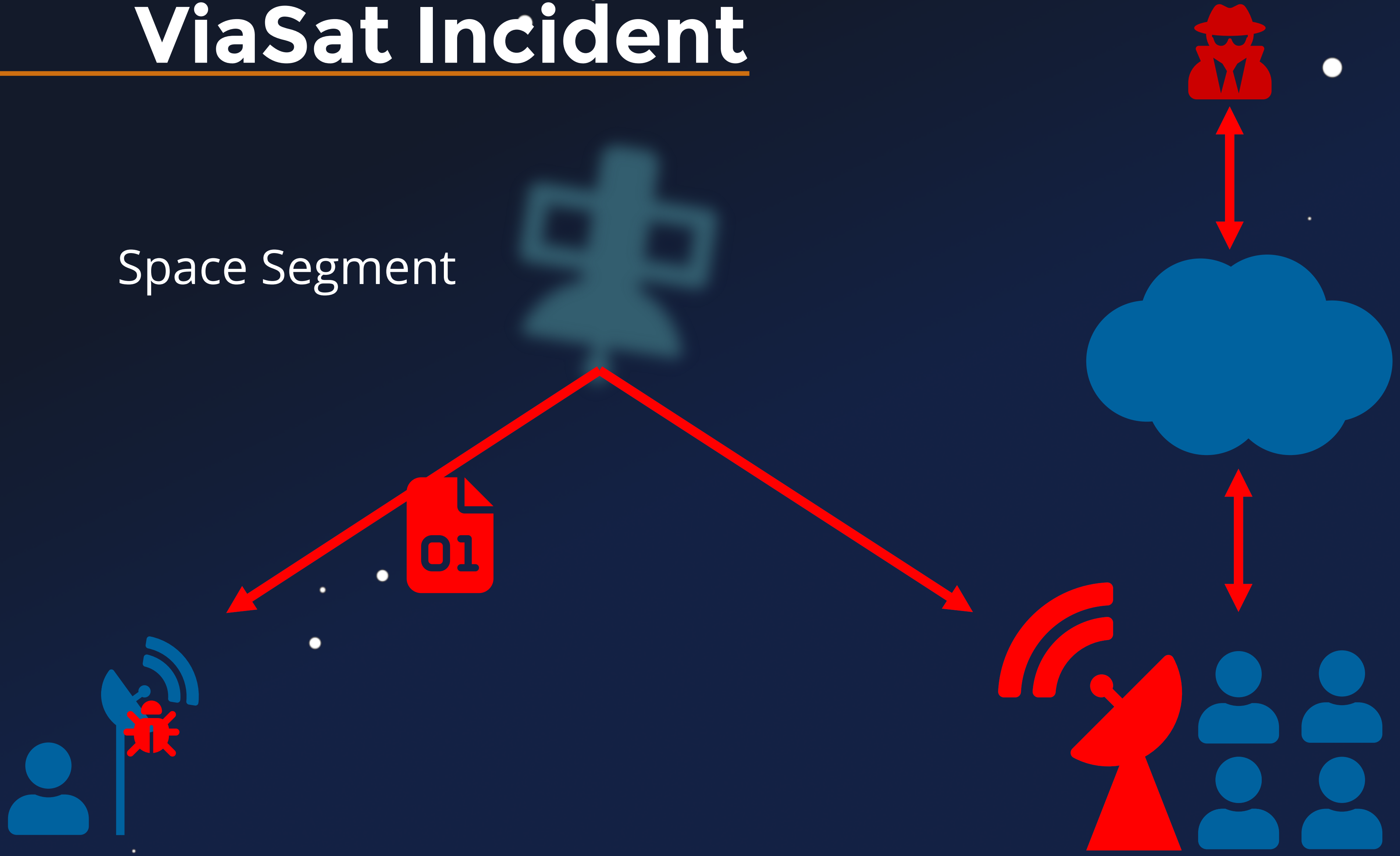
ViaSat Incident



ViaSat Incident



ViaSat Incident

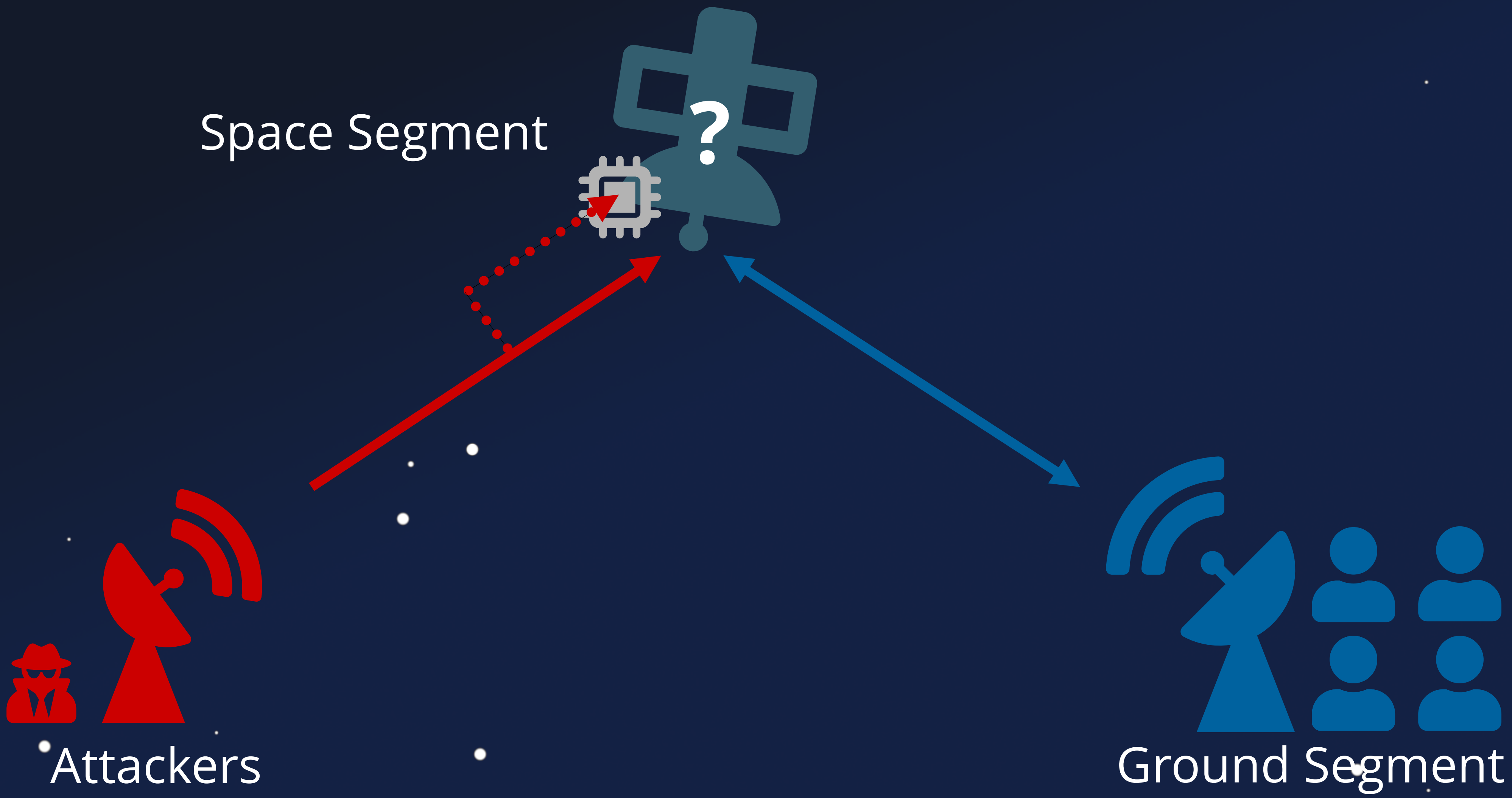


Space Segment

User Segment

Ground Segment

Firmware Attacks



Attacker Goals

Denial of Service

Attacker Goals

Denial of Service

Malicious Data Interaction

Attacker Goals

Denial of Service

Seizure of Control

Malicious Data Interaction

Attacker Goals

Denial of Service

Seizure of Control

Malicious Data Interaction

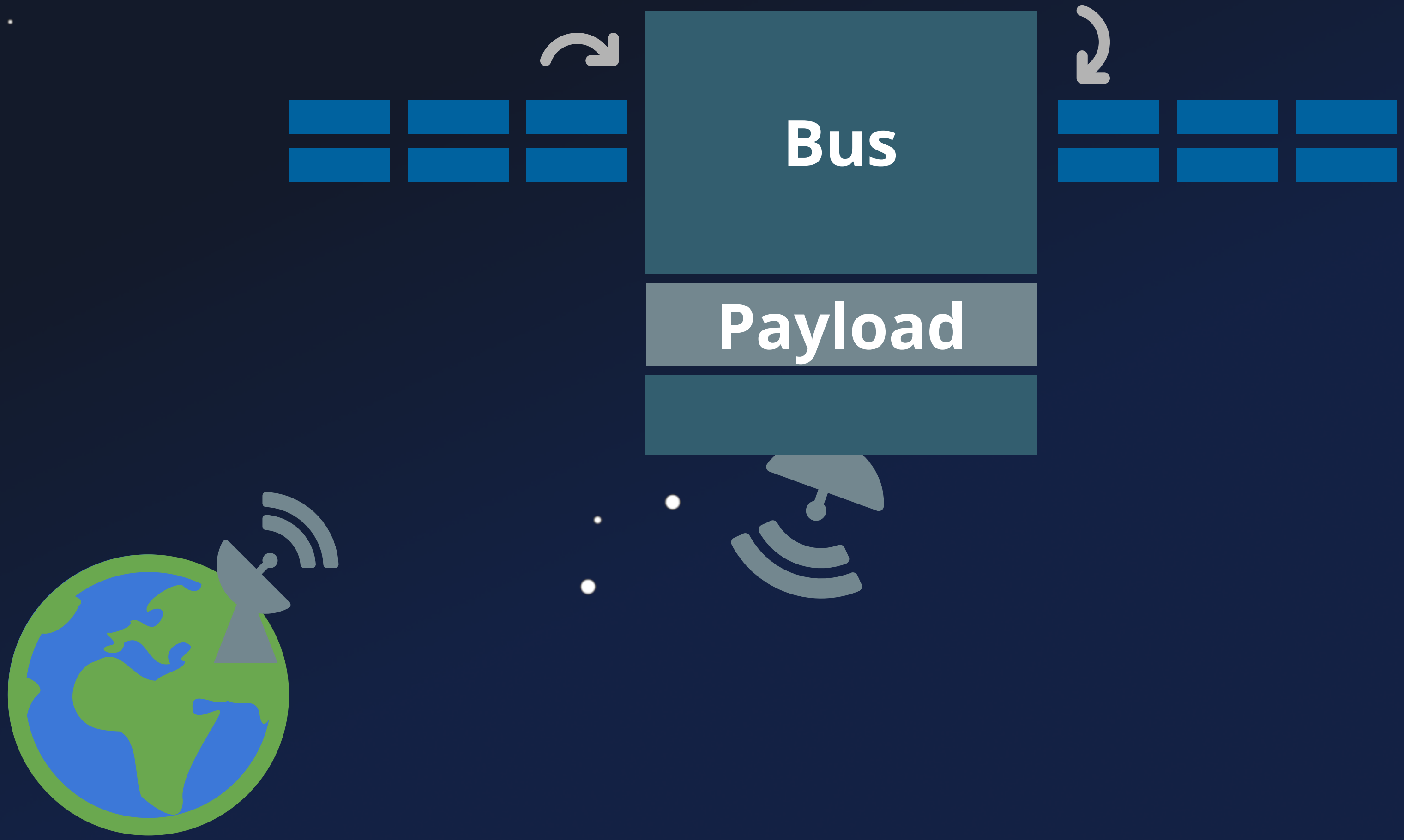
Attacker Goals

Seizure of Control

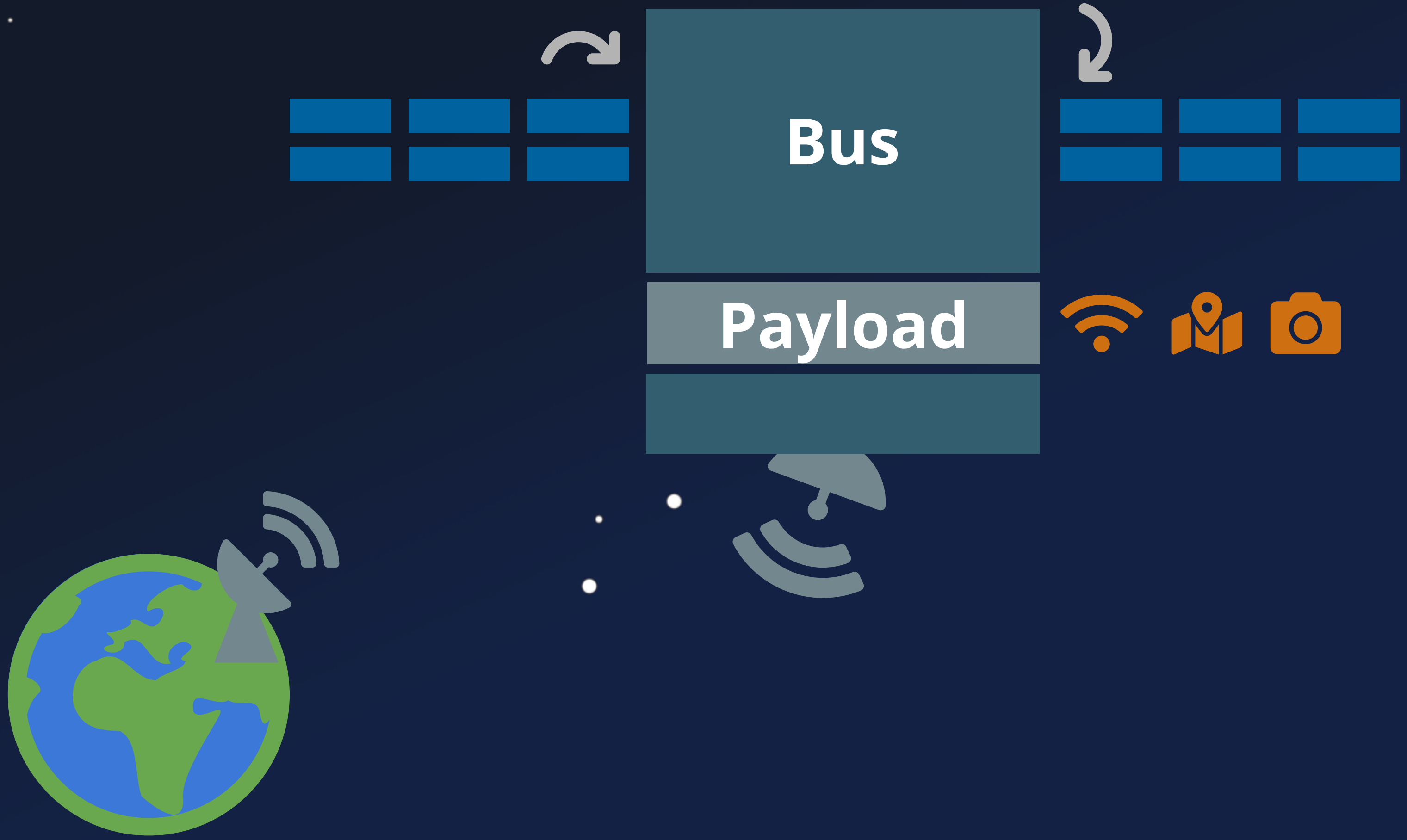
Attacker Goals

Seizure of Control

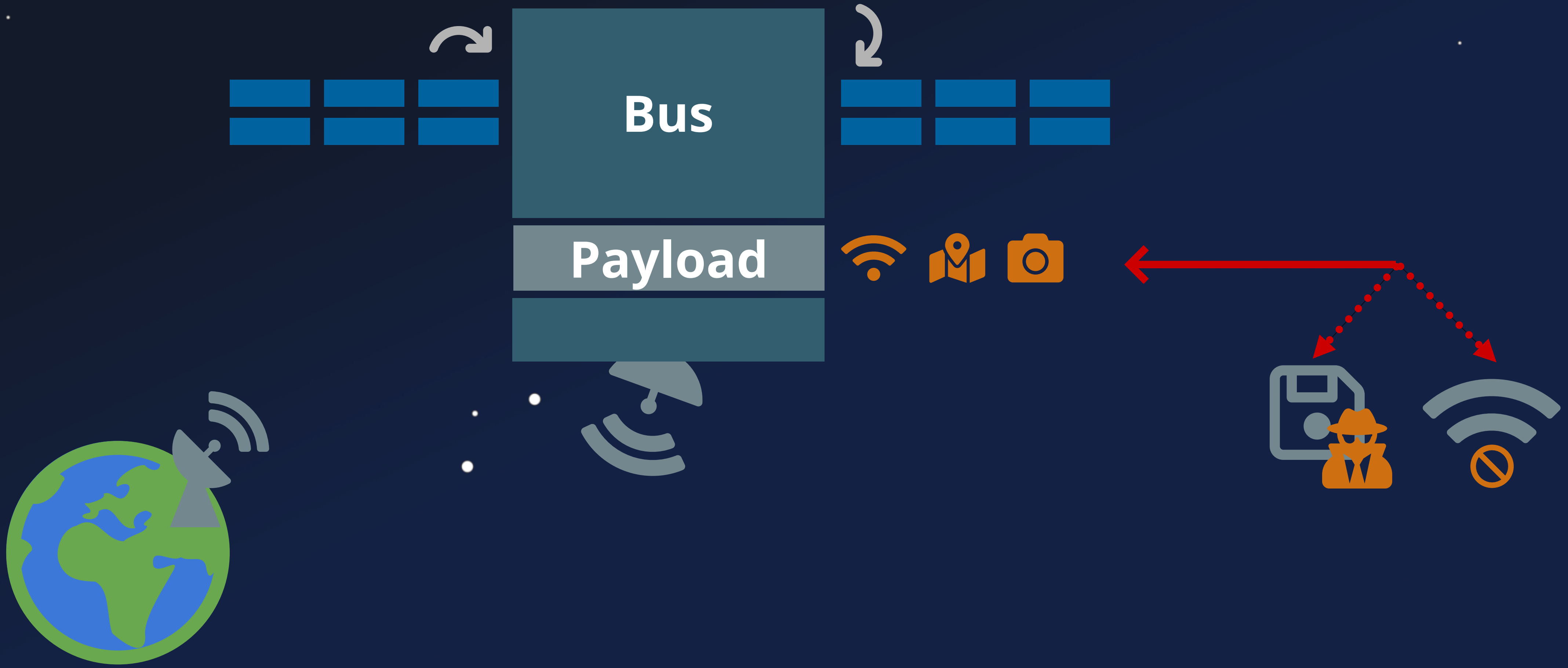
Components



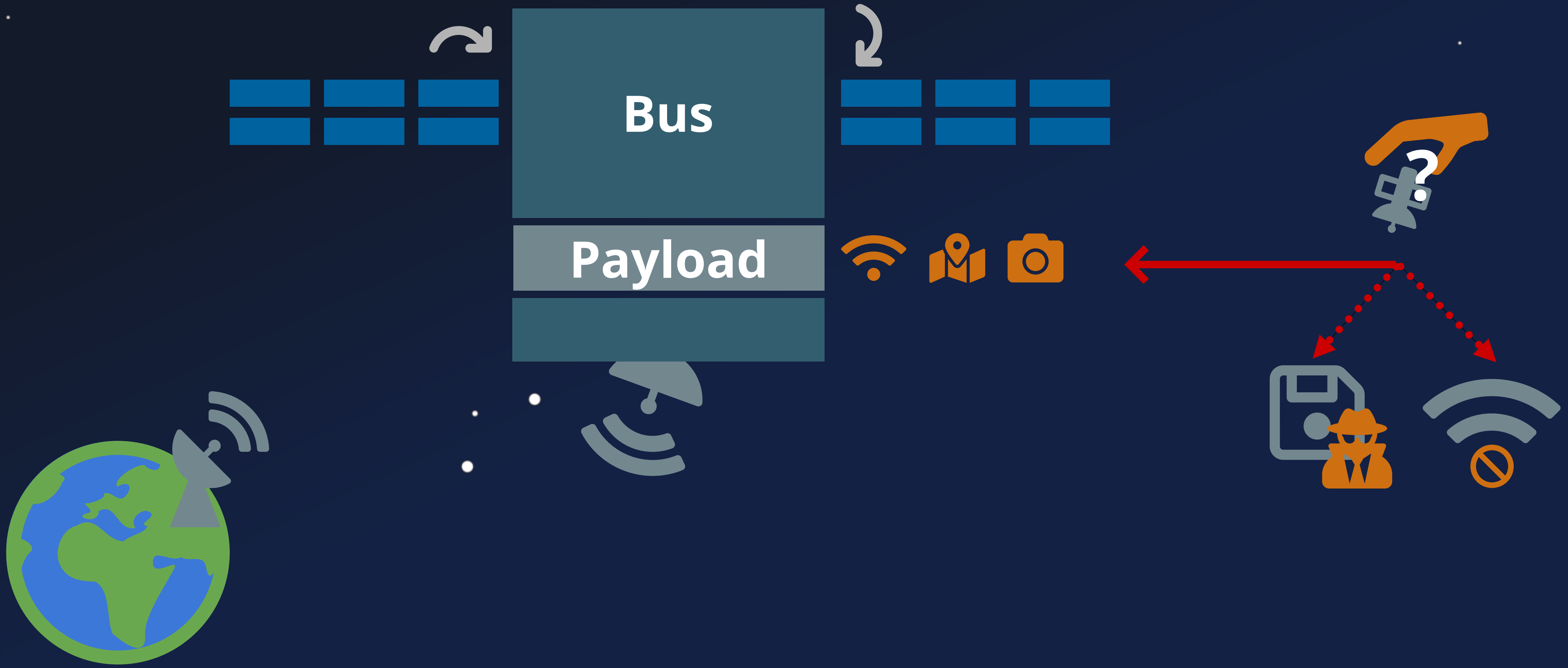
Components



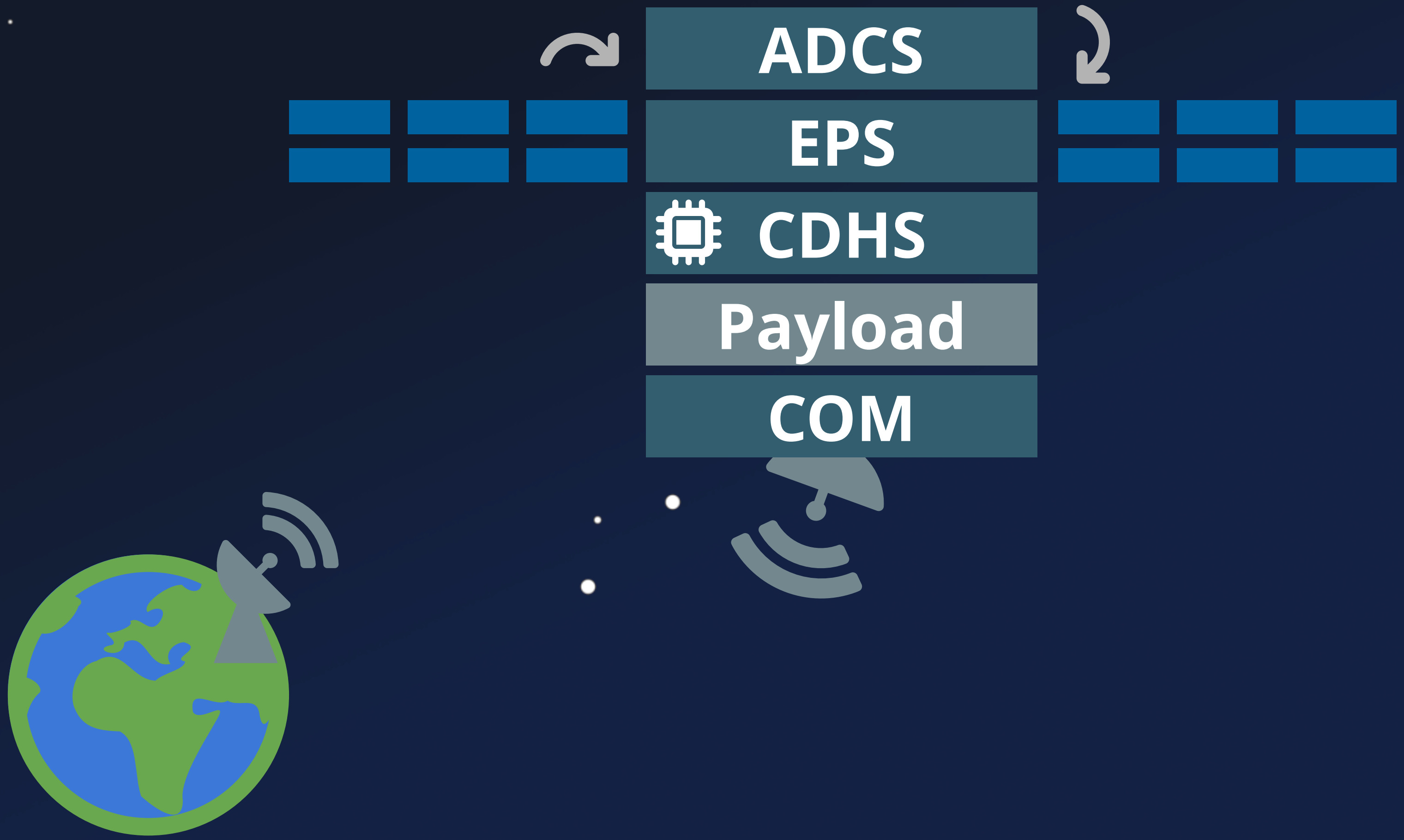
Components



Components



Components



ADCS

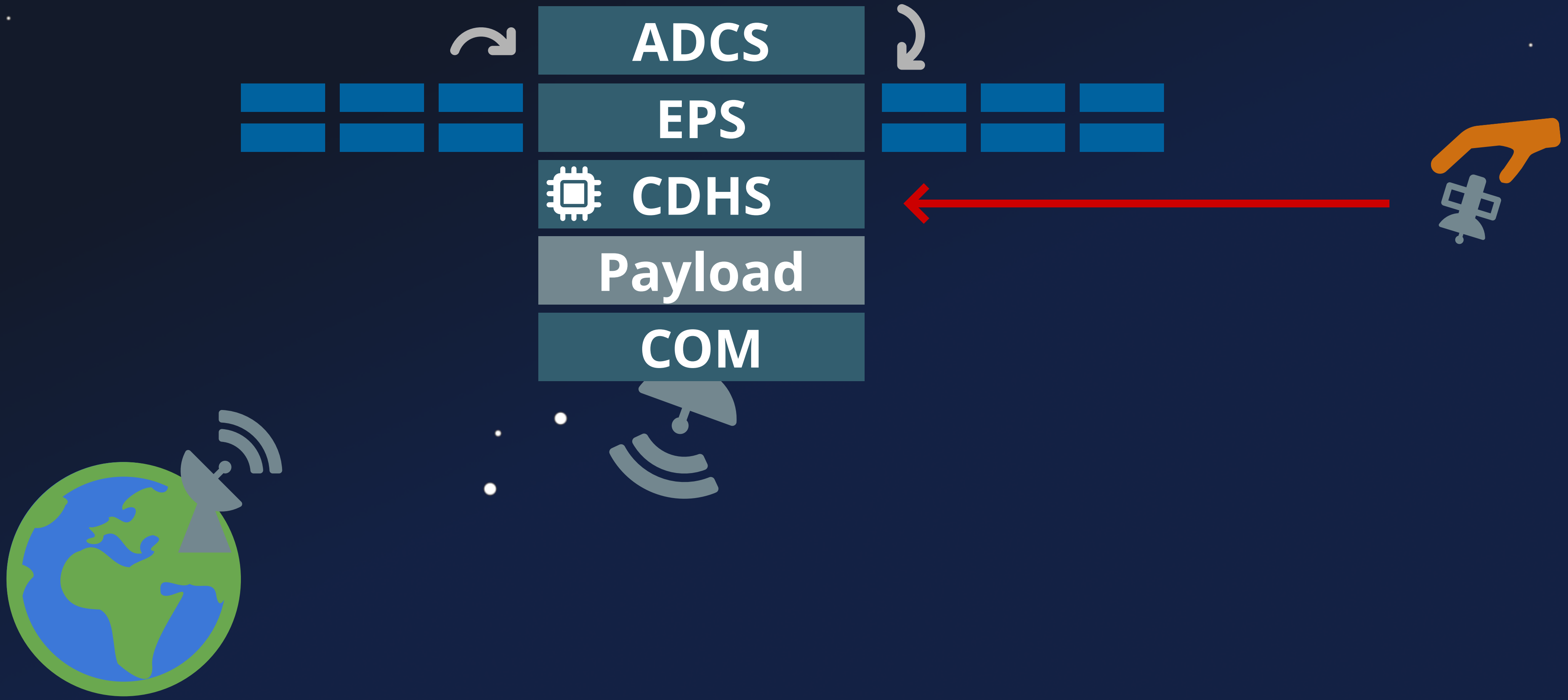
EPS

CDHS

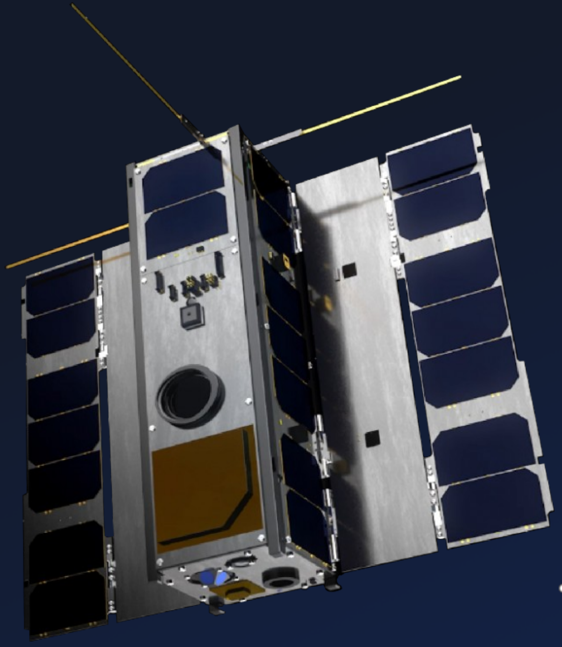
Payload

COM

Components



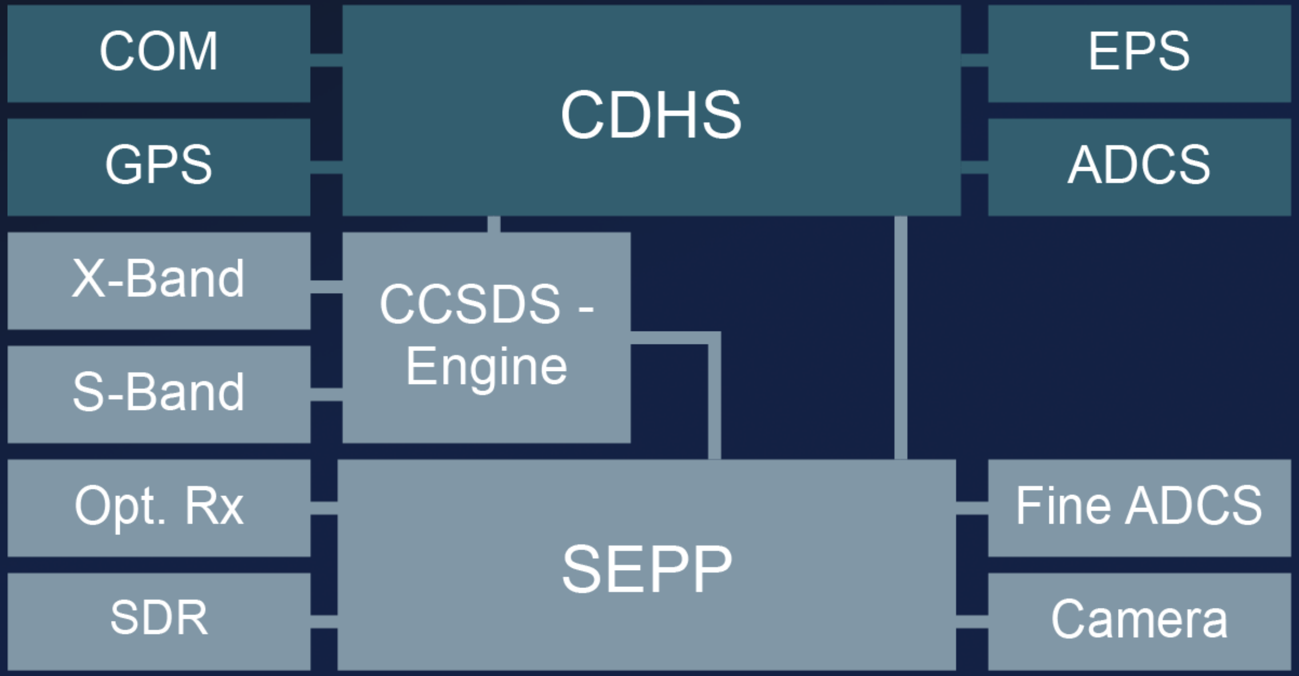
System Chart



Experimenter

Operated by ESA

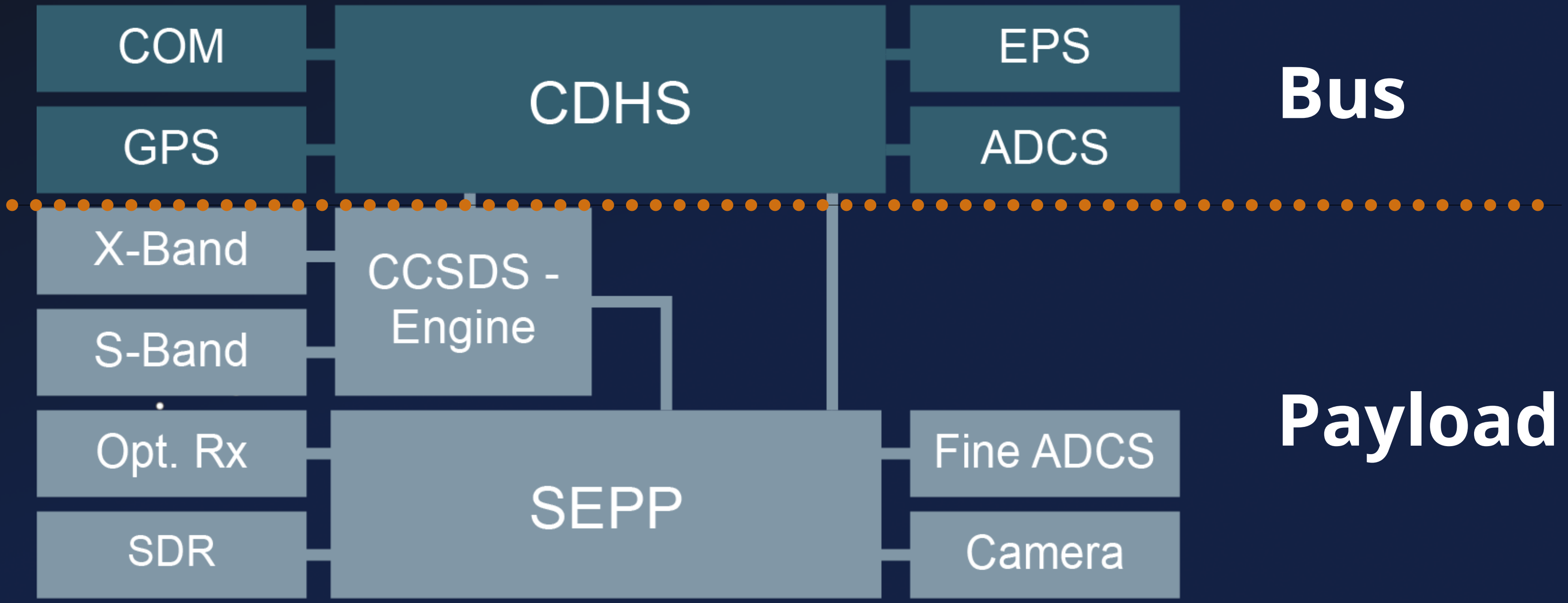
Open for Research



S-/X-Band, SDR, Optical Rx., Camera, ...

Peripherals

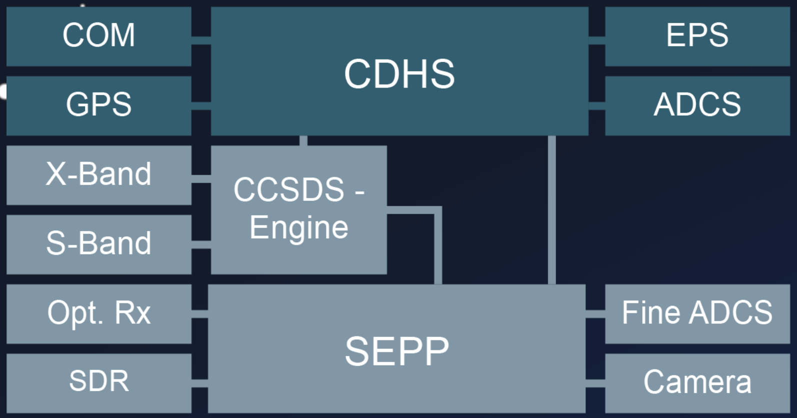
System Chart

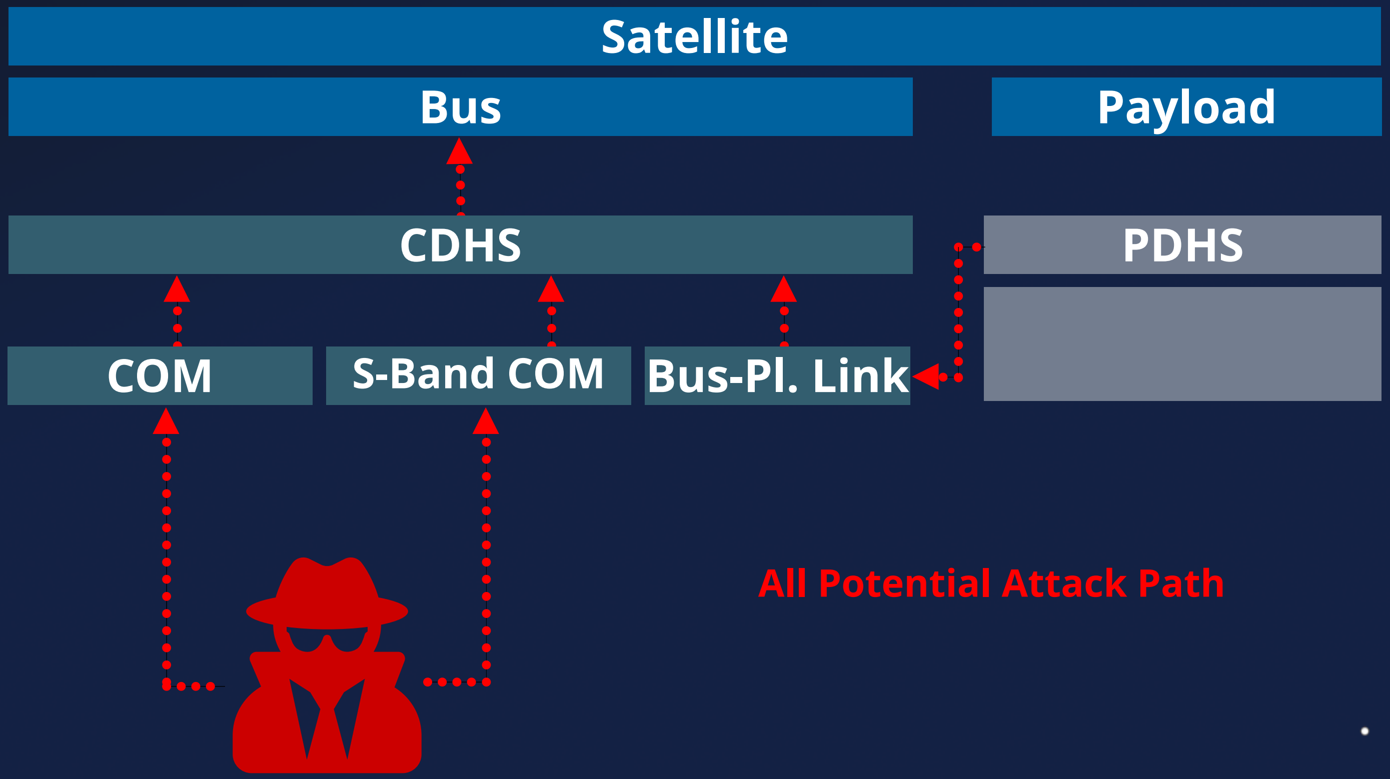


Bus

Payload

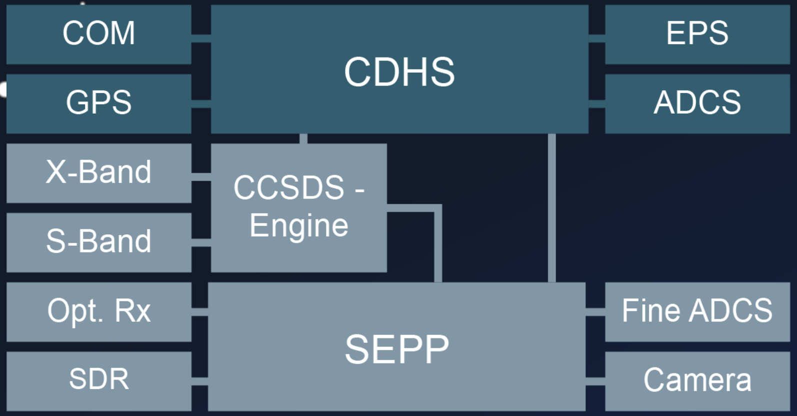
System Chart

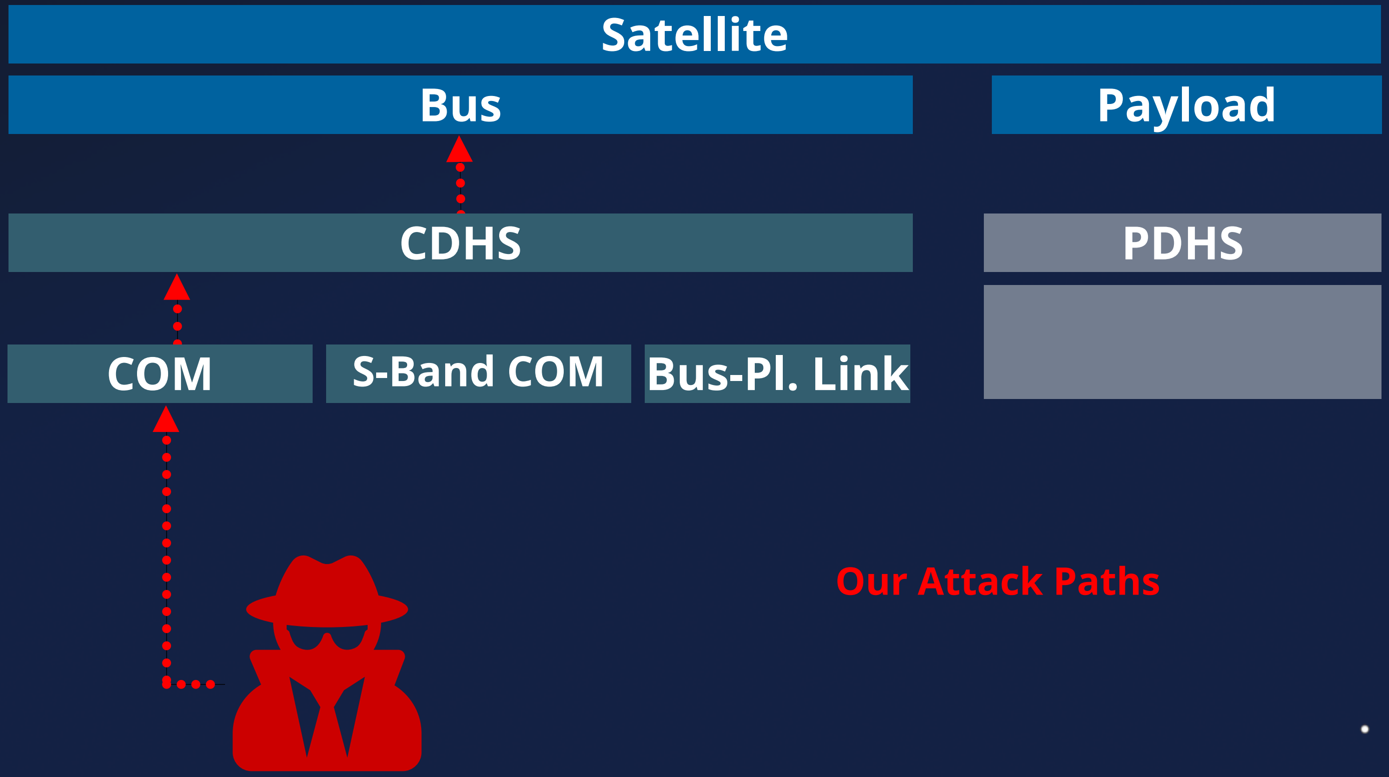




All Potential Attack Path

System Chart





OPS-Sat

COM

- Bypass Access Control
    - Missing Access Control

CDHS

- Vulnerable TC
    - Stack Buffer Overflow

Bus

- Arbitrary Code Execution
    - Missing OS Defenses

Satellite

OPS-Sat

COM

- Bypass Access Control
  - Missing Access Control

CDHS

- Vulnerable TC
  - Stack Buffer Overflow

Bus

- Arbitrary Code Execution
  - Missing OS Defenses

Satellite

Mission accomplished: Control seized

Developer Survey

Survey

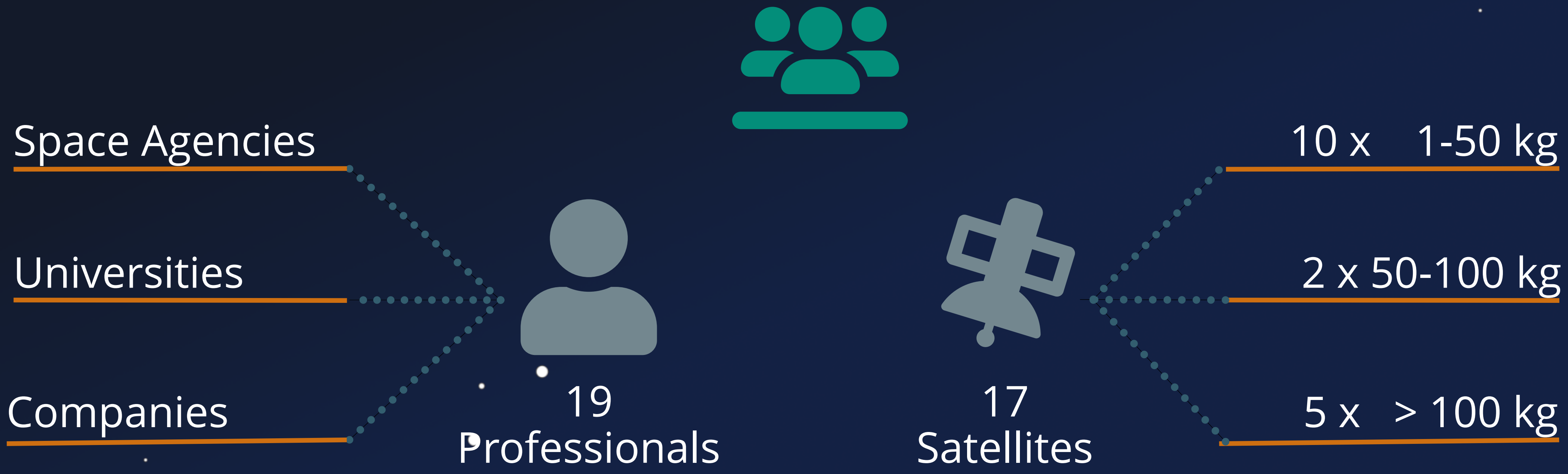
Space Agencies

Universities

Companies

19 Professionals

Survey



Space Agencies

Universities

Companies

19
Professionals

17
Satellites

10 x 1-50 kg

2 x 50-100 kg

5 x > 100 kg

Survey

Space Agencies

Universities

Companies

19 Professionals

17 Satellites

10 x 1-50 kg

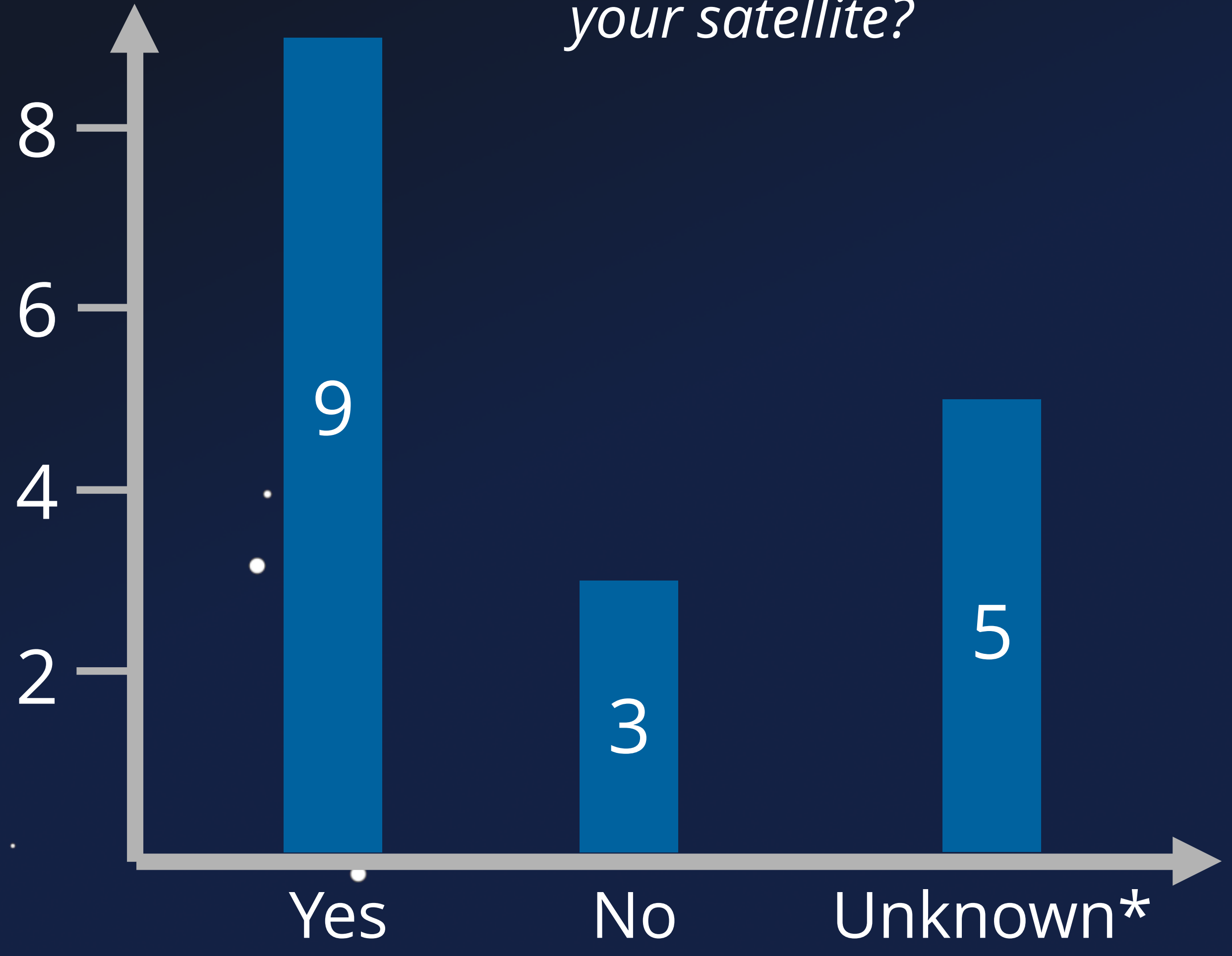
2 x 50-100 kg

5 x > 100 kg

Fully Anonymous

TC Protection

Question: *Are* ***any measures deployed*** *to prevent 3rd parties from controlling your satellite?*

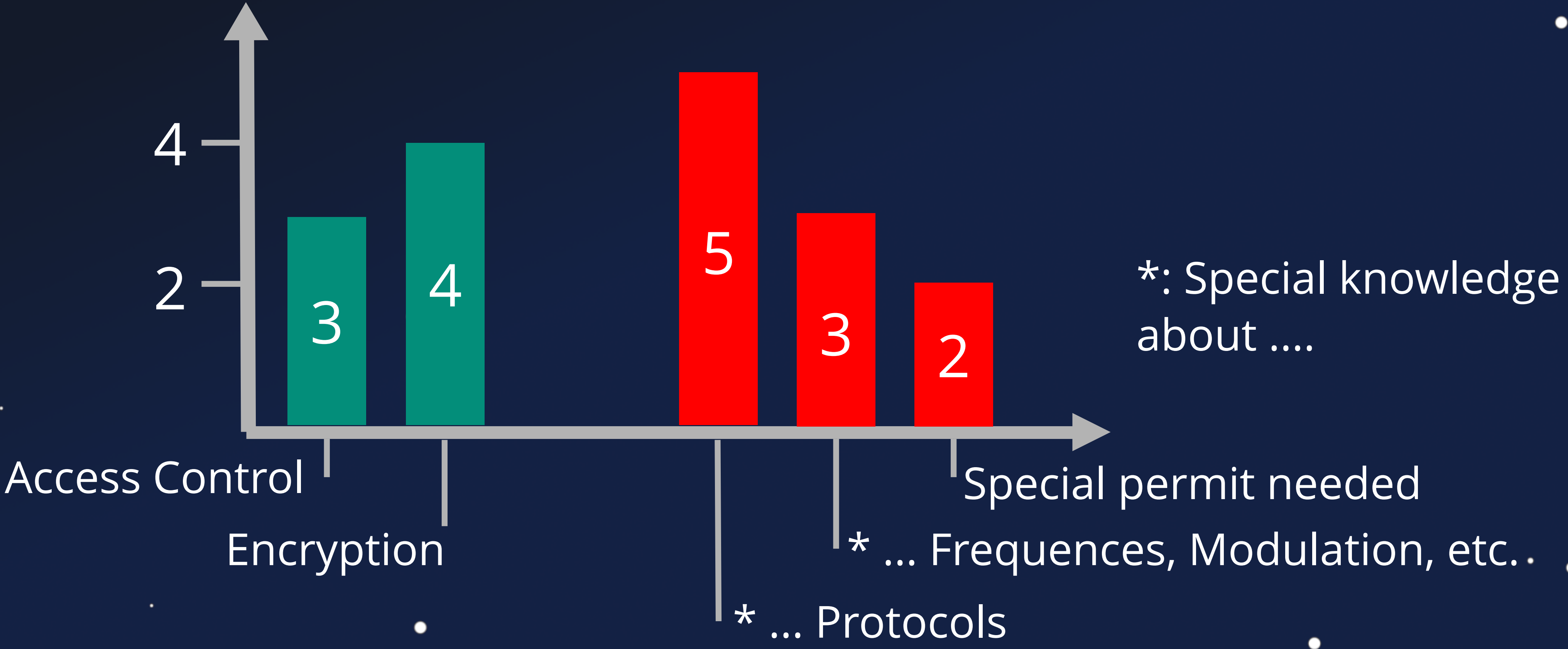


Unknown*:

Prefer not to say /
Don't know

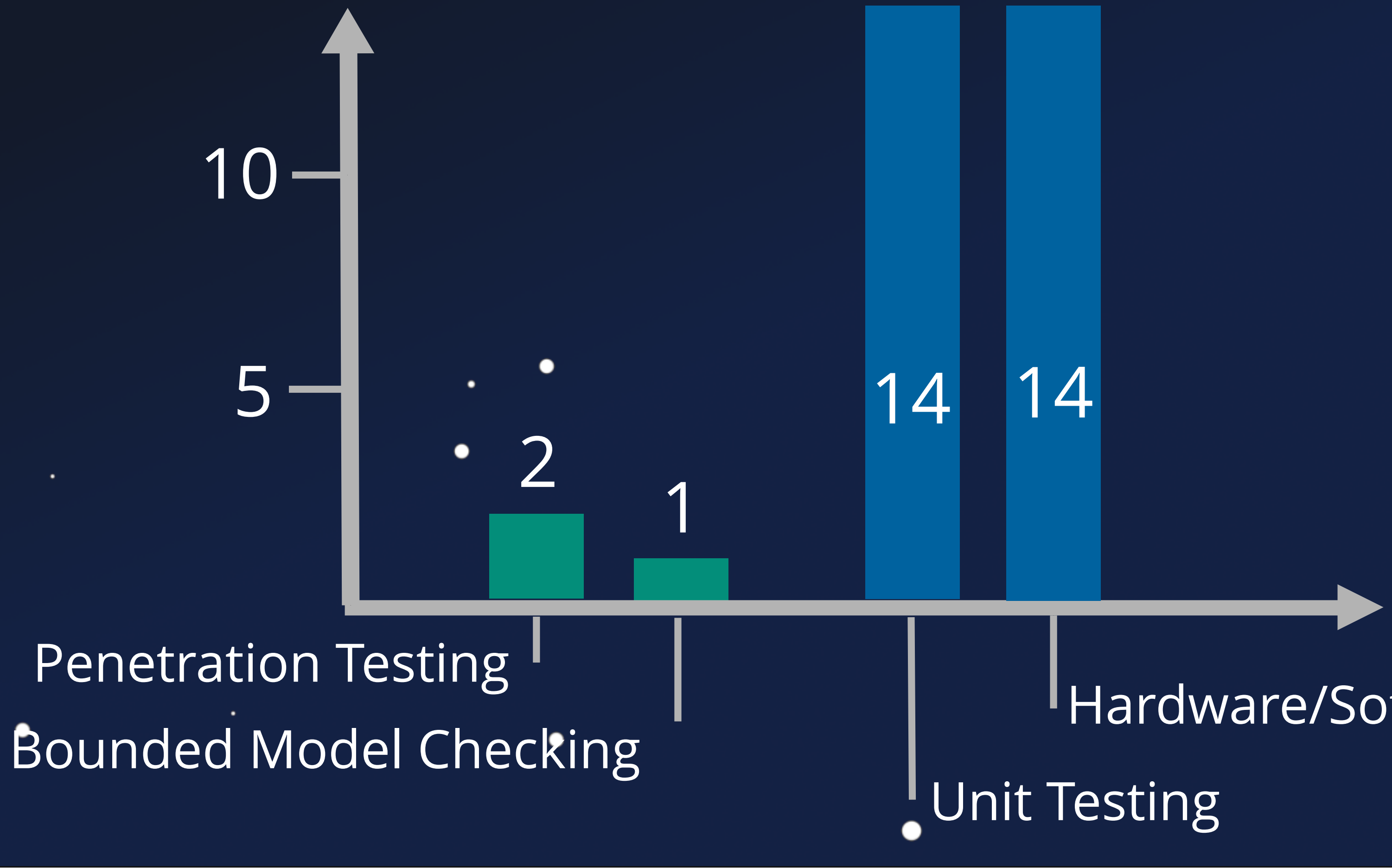
TC Obscurity

Question: ***What measures*** *are deployed to prevent 3rd parties from controlling your satellite? (Multiple Answers)*



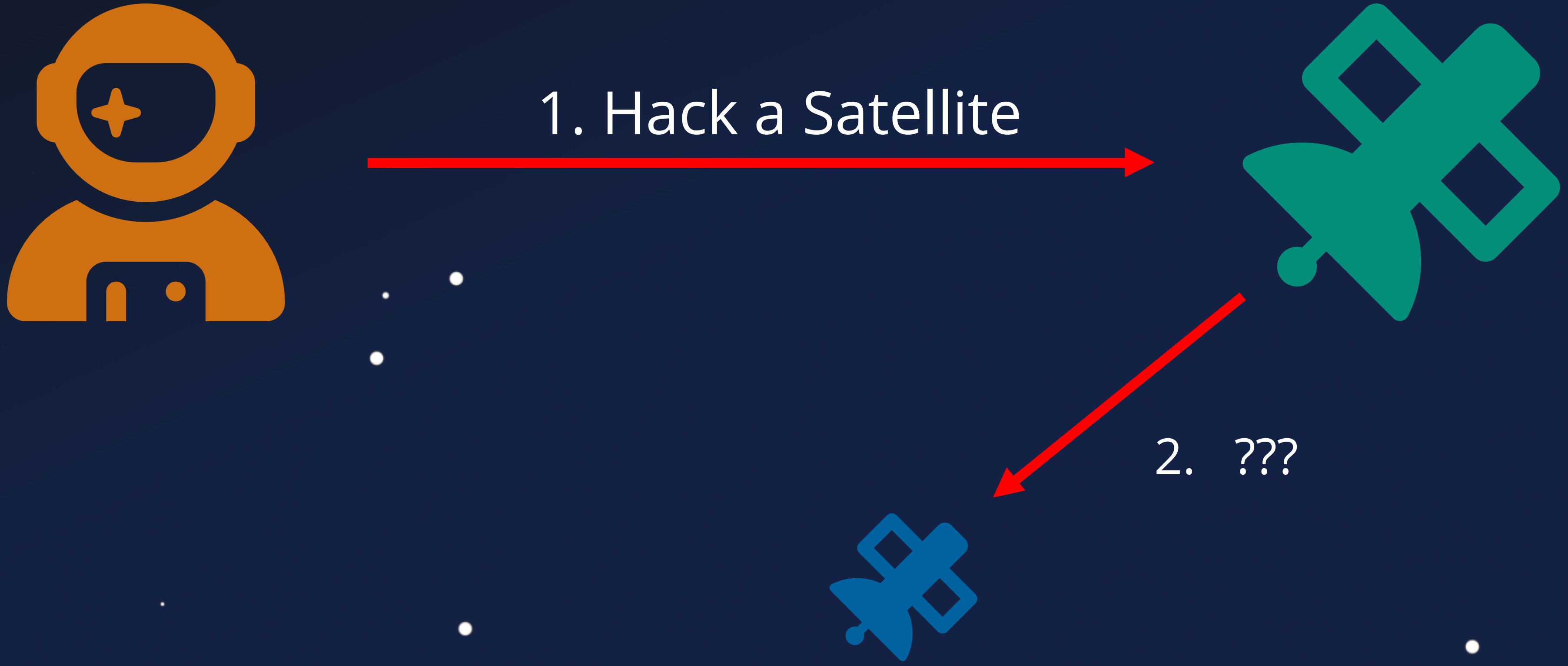
Security Testing

Question: ***Which***, *if any*, ***methods, tools or techniques*** *were used to ensure/improve code quality? (Multiple Answers Possible)*



“ But it's different for *my* satellite

Impact

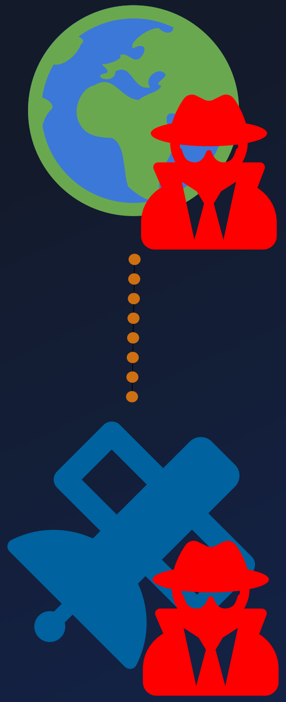


1. Hack a Satellite

2. ???

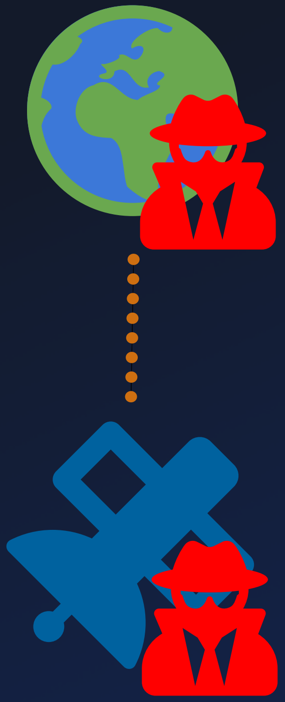
Scenarios

Scenarios



Orbital Access

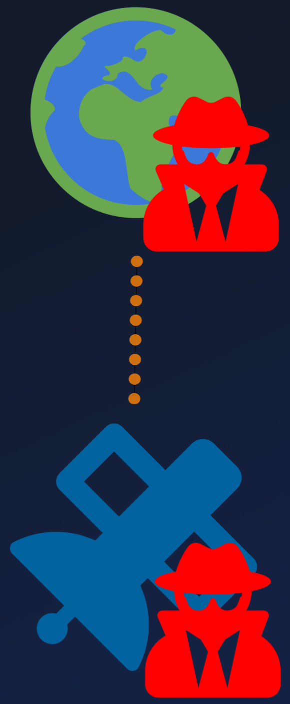
Scenarios



Orbital Access

1 Attacking Inter-Sat Links

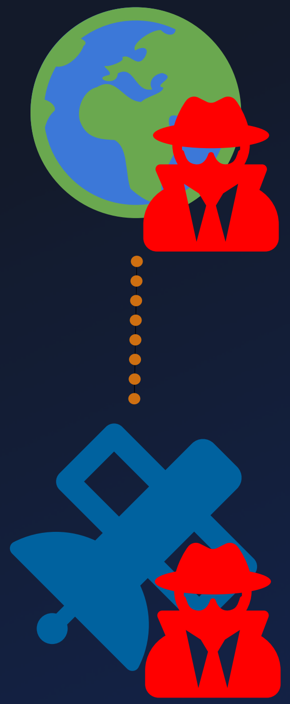
Scenarios



Orbital Access

1. Attacking Inter-Sat Links
2. Orbital Traffic Interception

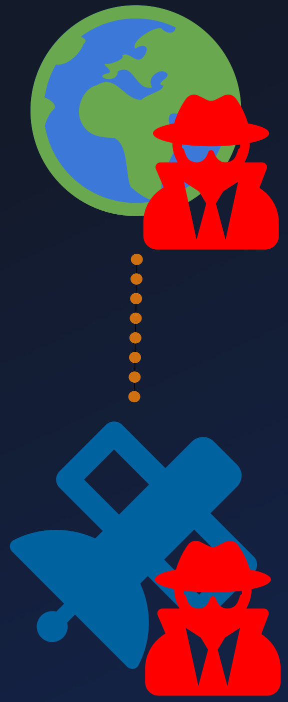
Scenarios



Orbital Access

1. Attacking Inter-Sat Links
2. Orbital Traffic Interception
3. Orbital Denial-of-Service

Scenarios



Orbital Access

1. Attacking Inter-Sat Links
2. Orbital Traffic Interception
3. Orbital Denial-of-Service
4. Kessler Syndrome

Attacker Perspective

Hack-a-Sat

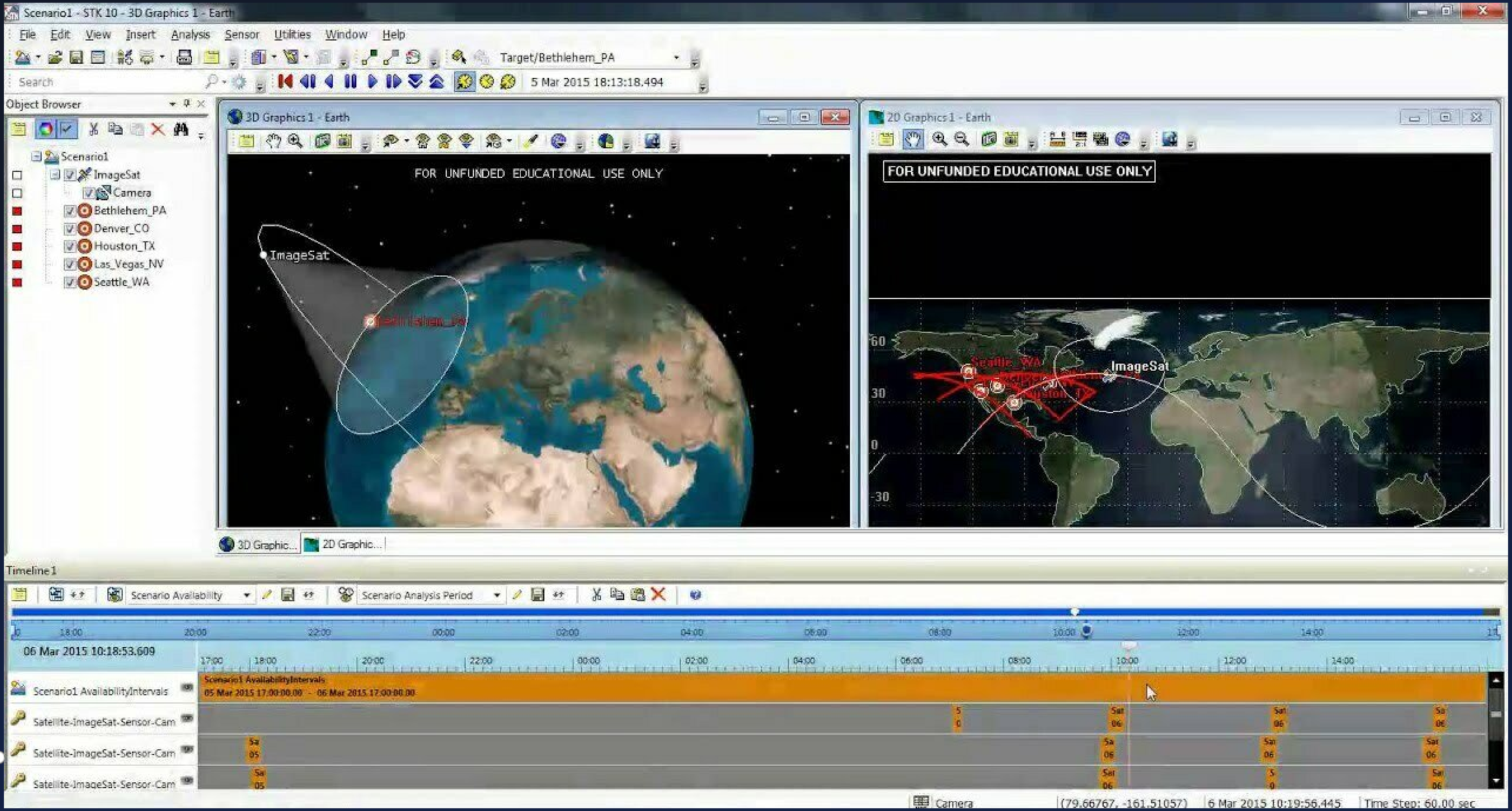
HACK-A-SAT
010
2
THE GOOD, THE BAD
AND THE CYBER-SECURE

010
4

*** Flux *** Repeat *** Rocket ***

KRAUT
SAT

Math? Math!



Target/Bethlehem_PA

5 Mar 2015 18:13:18.494

Scenario Availability

Scenario Analysis Period

06 Mar 2015 10:18:53.609

Scenario1 AvailabilityIntervals
05 Mar 2015 17:00:00.00 - 06 Mar 2015 17:00:00.00

(79.66767, -161.51057) | 6 Mar 2015 10:19:56.445 | Time Step: 60.00 sec

HACK-A-SAT CONTACT WINDOW TIMELINE

▲ Contact Window Deadline for Team Submissions

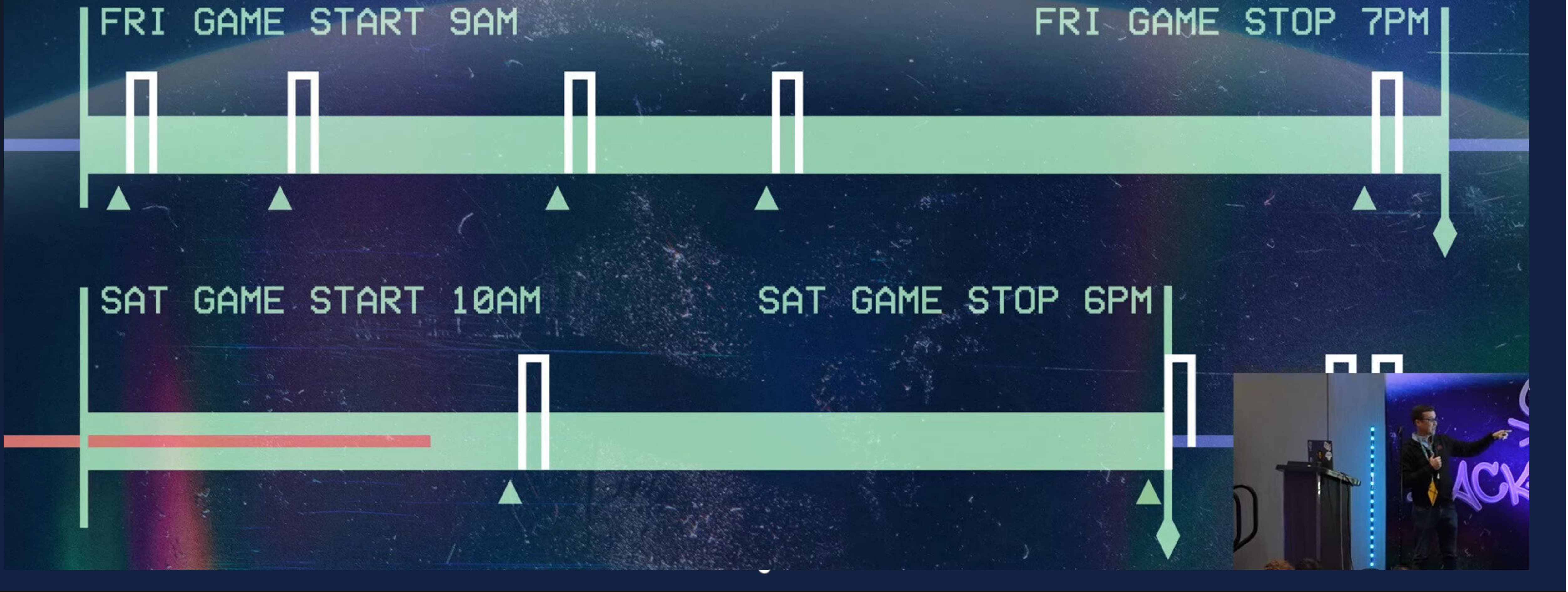
◆ Overnight Deadline for Team Submissions

□ Contact Window

🟩 Game Hours

🟦 Off Hours

🟥 ACS



FRI GAME START 9AM

FRI GAME STOP 7PM

SAT GAME START 10AM

SAT GAME STOP 6PM

Q&A

- Firmware Attacks on Satellites
- Satellite Exploitation Objectives
- Satellite Developer Survey
- Attacker Perspective

@jwillbold

/jwillbold

Johannes Willbold - johannes.willbold@rub.de