

# HoneySat: A Network-based Satellite Honey-pot Framework

*Efrén López-Morales\*, Ulysse Planta\*, Gabriele Marra, Carlos González, Jacob Hopkins,  
Majid Garoosi, Elías Obreque, Carlos Rubio-Medrano, Ali Abbasi*

*\*Equal Contribution*

Ulysse Planta





# Deception with Honeypots

- **Lures attackers** into controlled, instrumented decoys
- **High-interaction “mission realism”**: Real ground tools + realistic interfaces
- Detecting presence (and methods) of Attackers
- Honeypots often mimic key behaviors, not the full real system
- **We need a realistic decoy that doesn't require mission-specific internals and doesn't reveal how the real mission works**



# Motivation



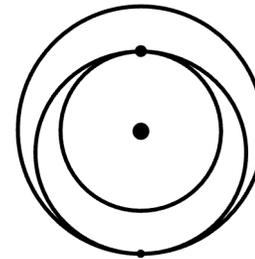
**Viasat KA-SAT**

Feb. 2022

**APT** Targeting  
Multiple Companies

**TIDRONE**

Sep. 2024



**STARLINK**

**Starlink Infrastructure  
Breach Attempts**

Early 2025



**GPS Spoofing**

Aug. 2025



# Motivation

- **RoSAT** X-ray astronomy satellite launched in 1990



# Motivation

- **RoSAT** X-ray astronomy satellite launched in 1990
- **Instrument damage associated with Sun exposure/pointing issues,** followed by shutdown in **1999**



# Motivation

- **RoSAT** X-ray astronomy satellite launched in 1990
- **Instrument damage associated with Sun exposure/pointing issues**, followed by shutdown in **1999**
- A **network intrusion** into systems associated with NASA/GSFC was **documented**



# Motivation

- **RoSAT** X-ray astronomy satellite launched in 1990
- **Instrument damage associated with Sun exposure/pointing issues**, followed by shutdown in **1999**
- A **network intrusion** into systems associated with NASA/GSFC was **documented**
- **Permanent damage to onboard systems**



# Motivation

- **RoSAT** X-ray astronomy satellite launched in 1990
- **Instrument damage associated with Sun exposure/pointing issues**, followed by shutdown in **1999**
- A **network intrusion** into systems associated with NASA/GSFC was **documented**
- **Permanent damage to onboard systems**
- **How are these incidents connected?**



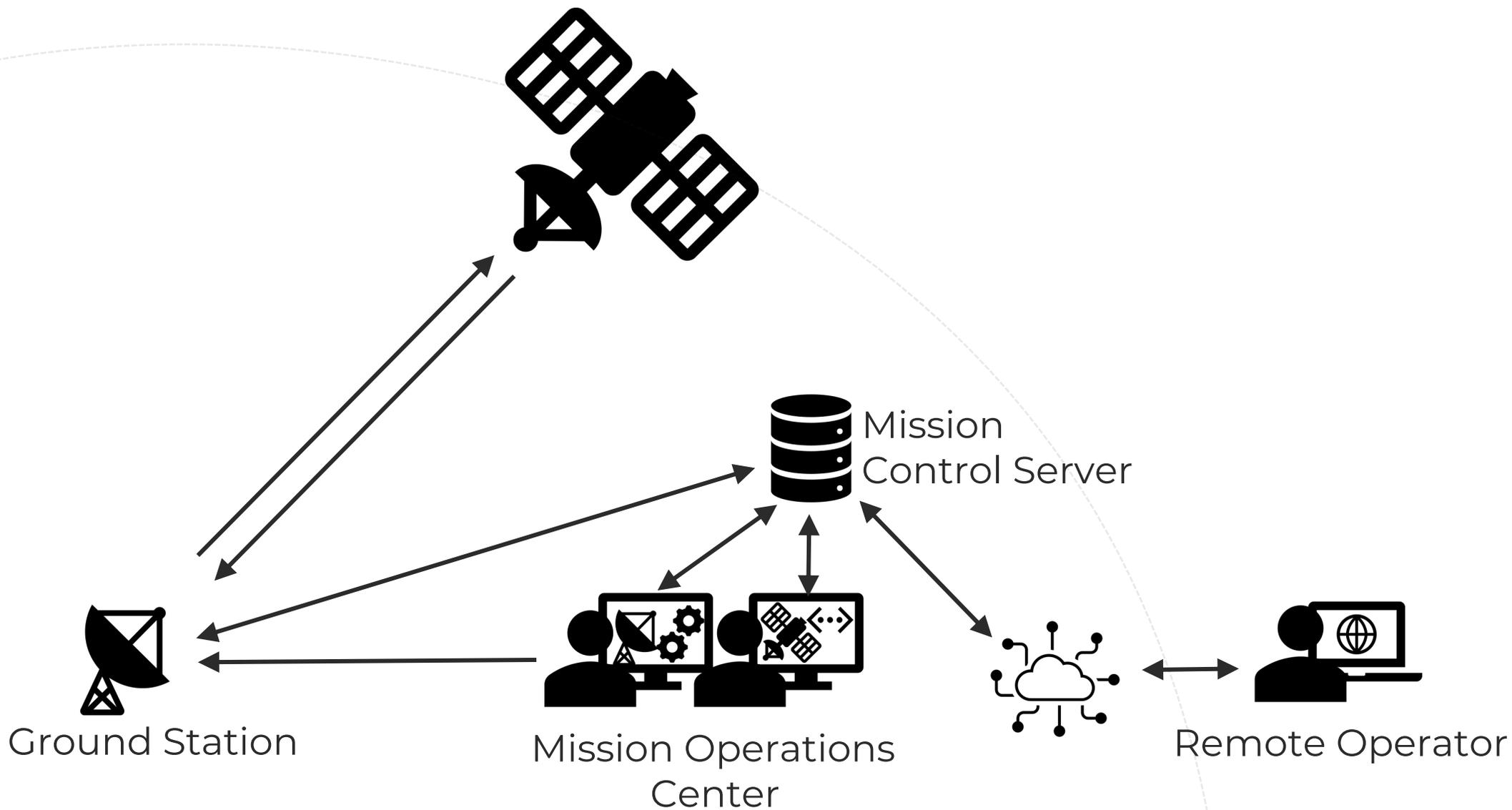
# Objectives

*Design Objectives of a Satellite  
Honeypot*

- I. Capture Rich interaction Data
- II. Deception
- III. Extensibility and Customizability

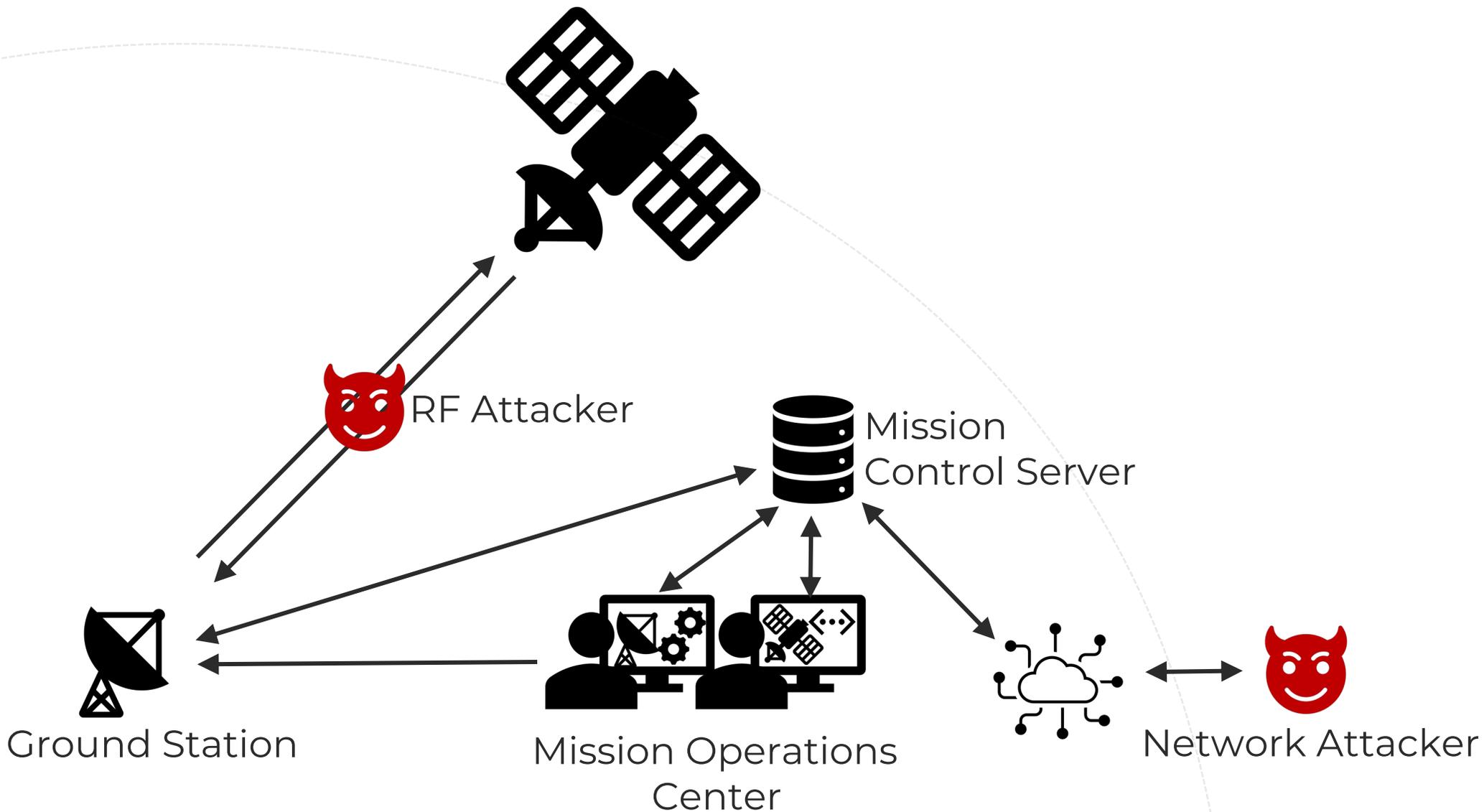


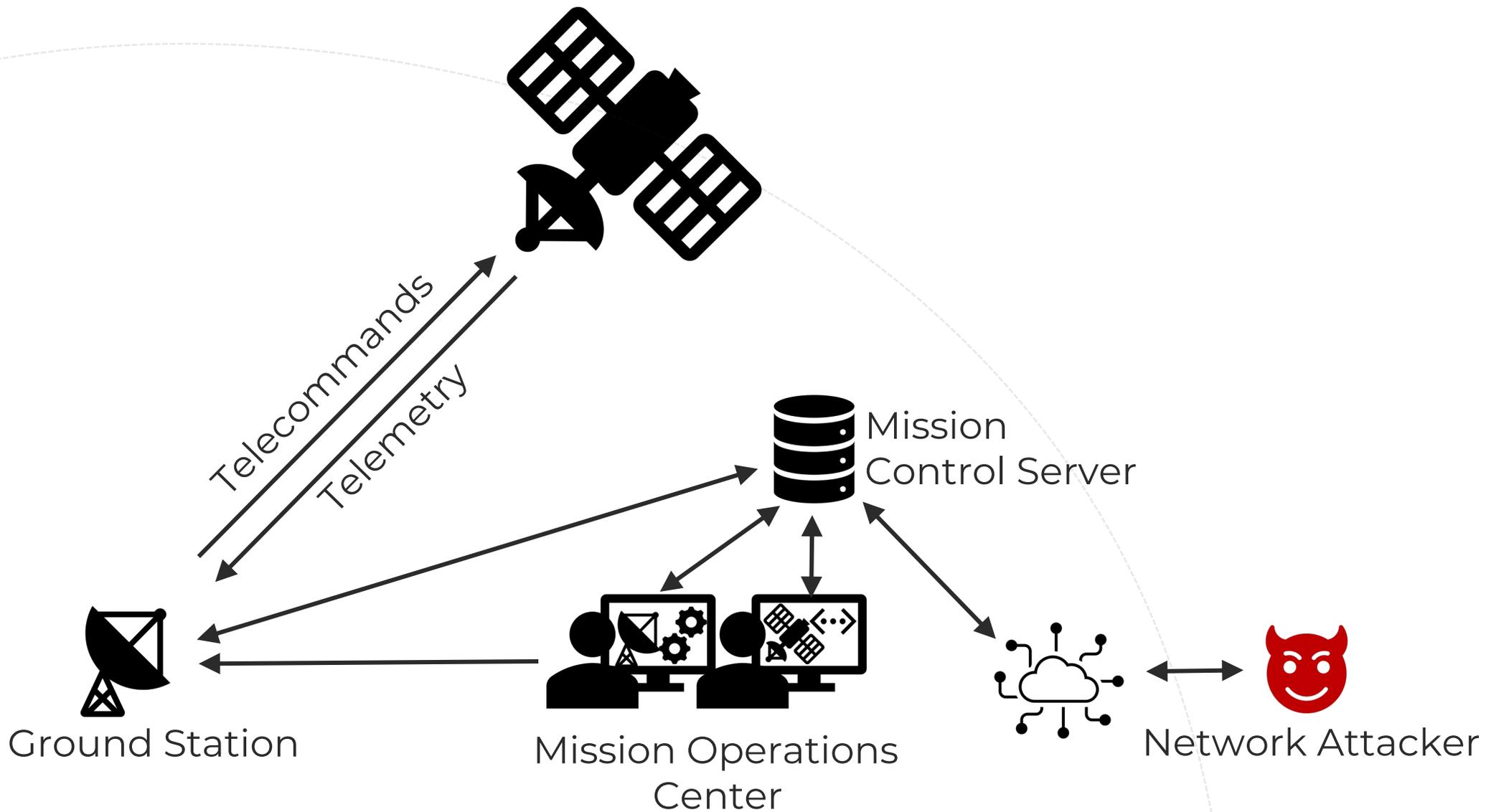
# Overview

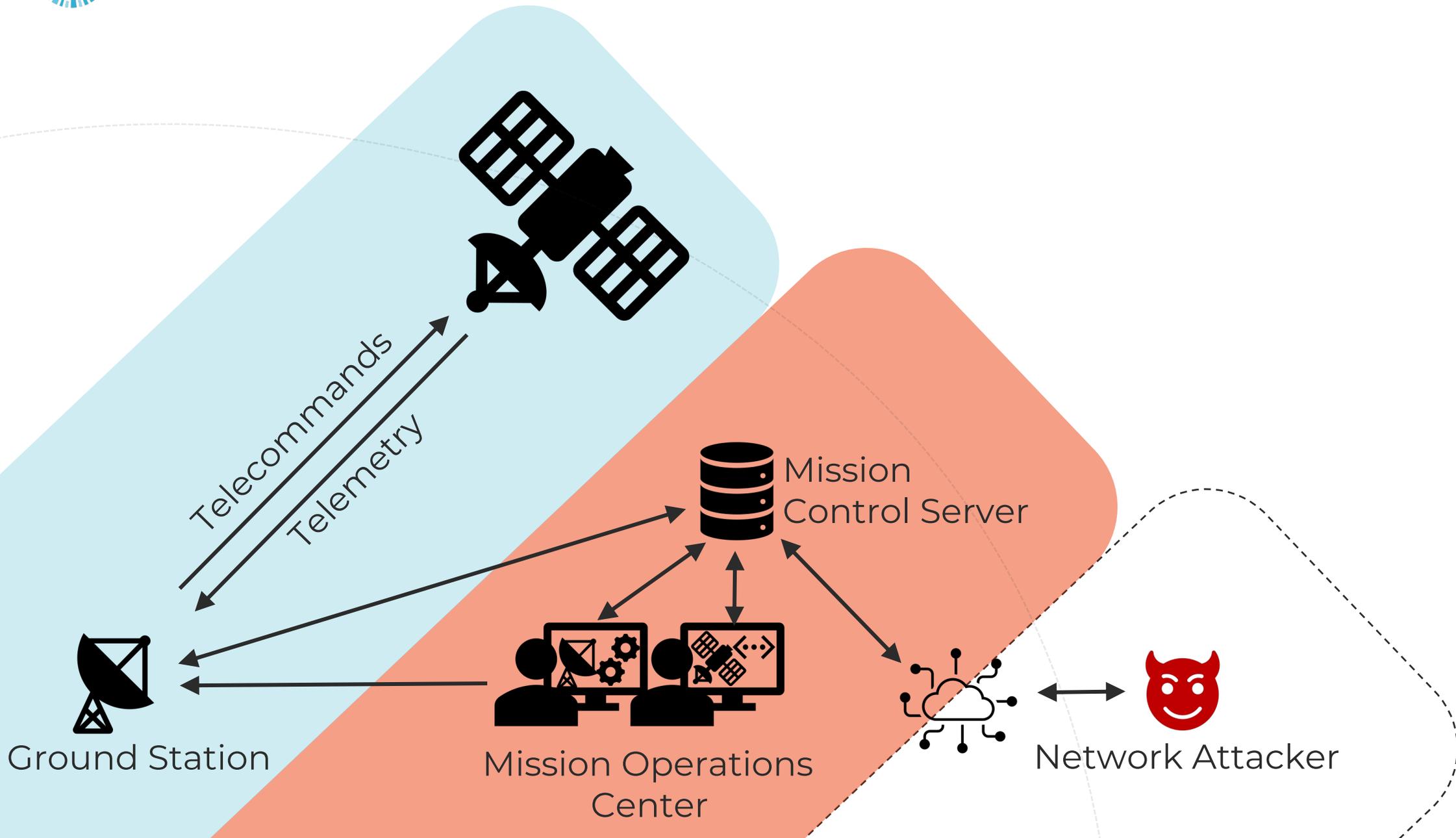




# Attacker Model

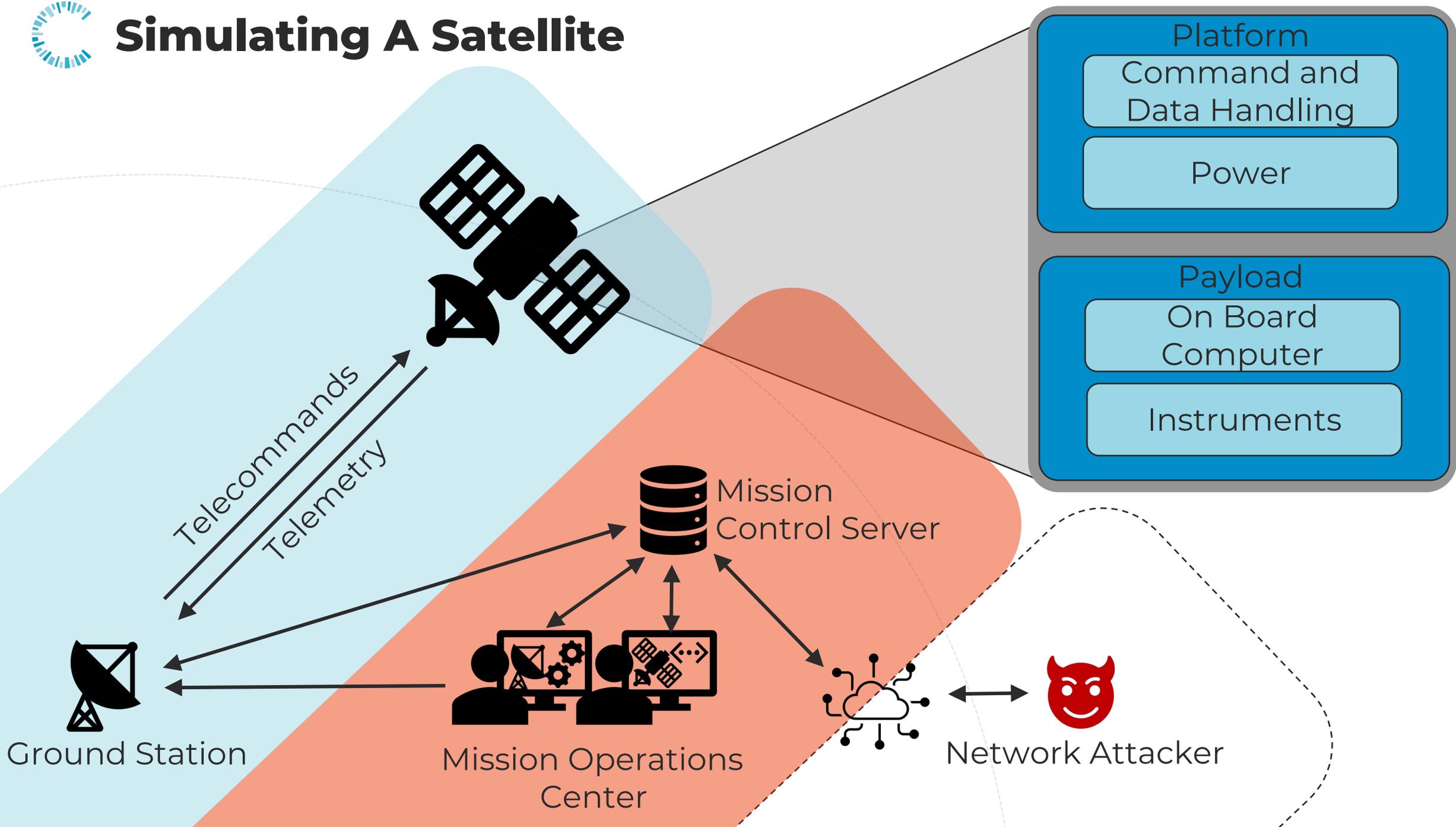






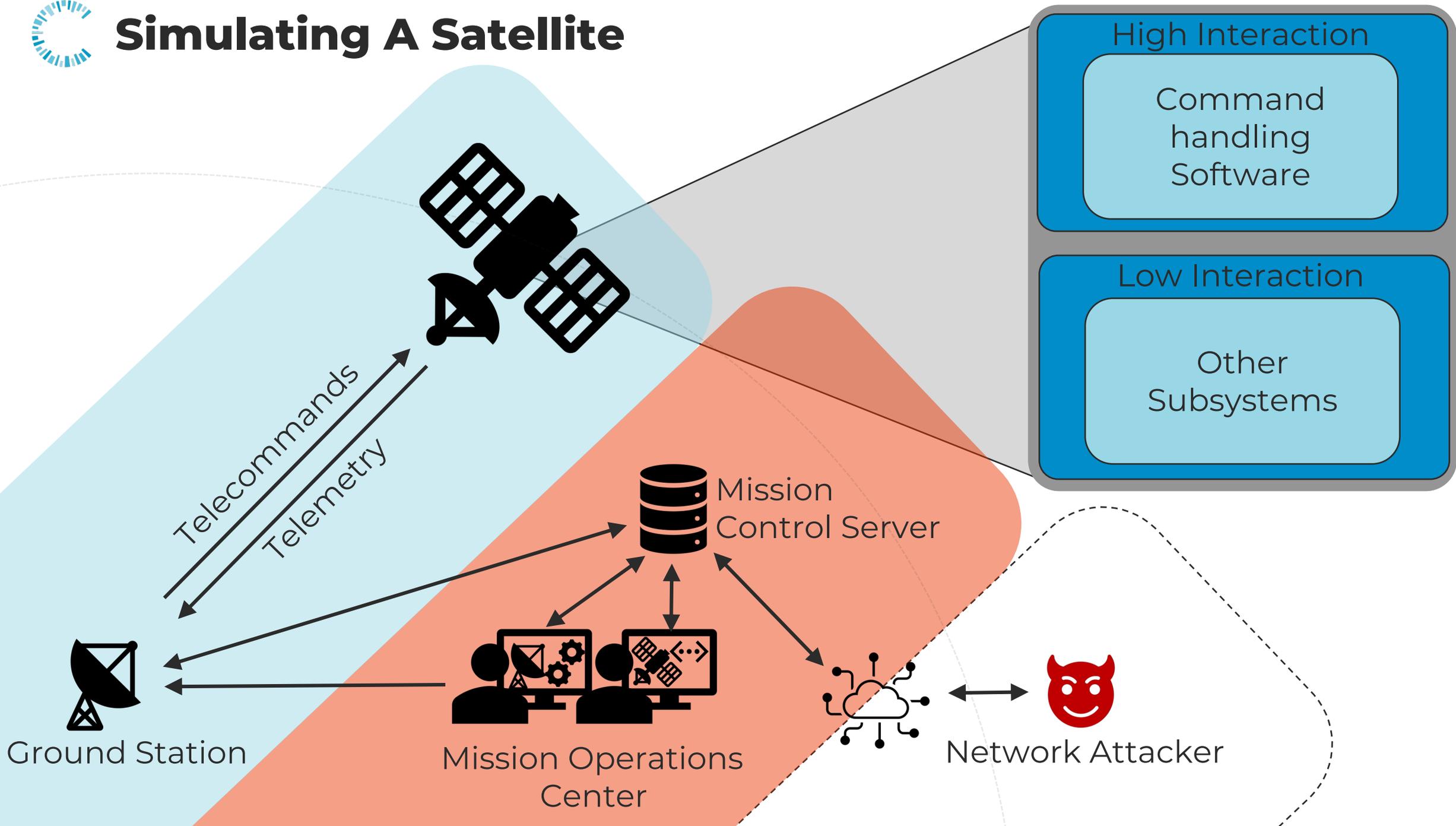


# Simulating A Satellite



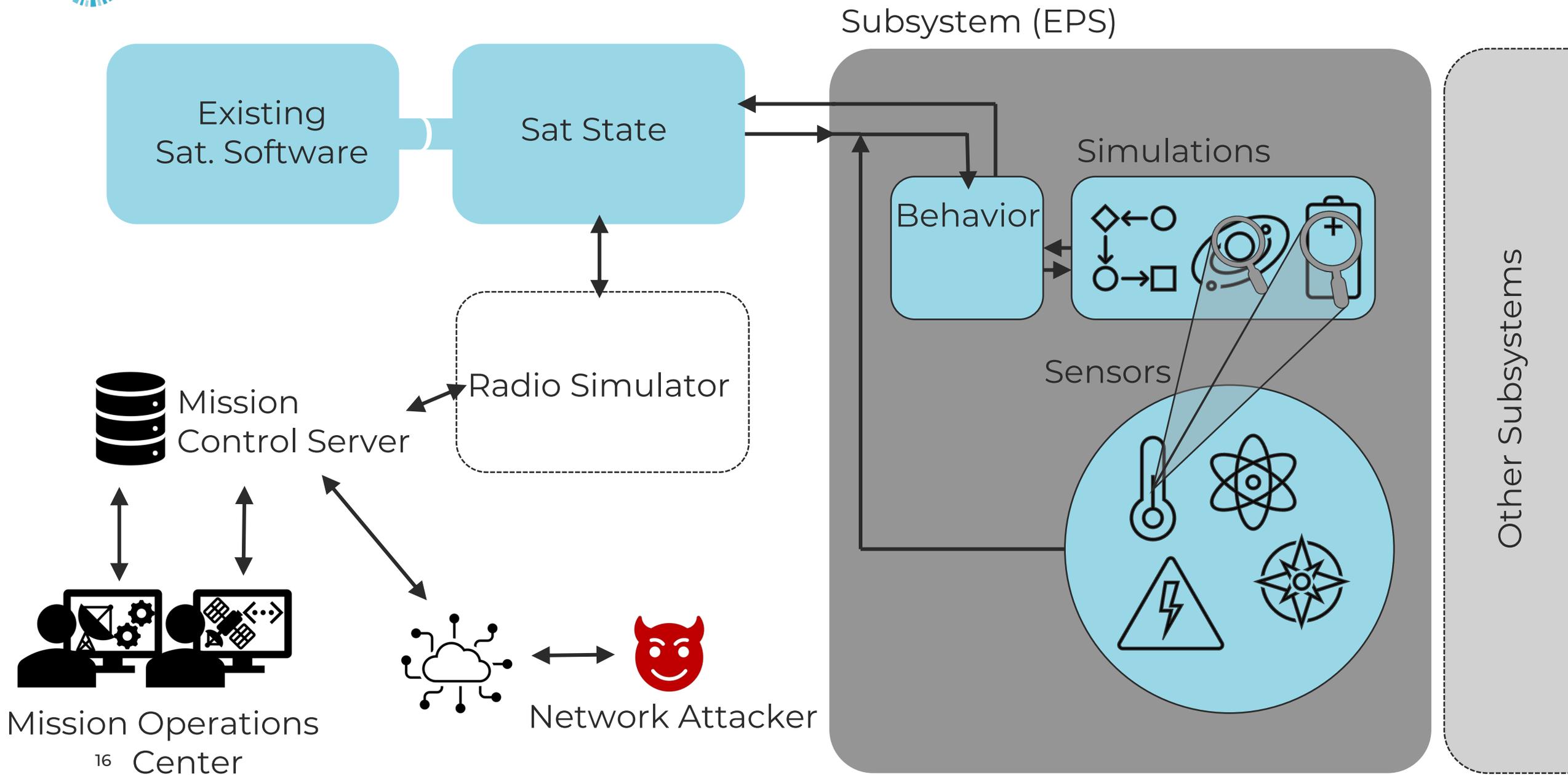


# Simulating A Satellite



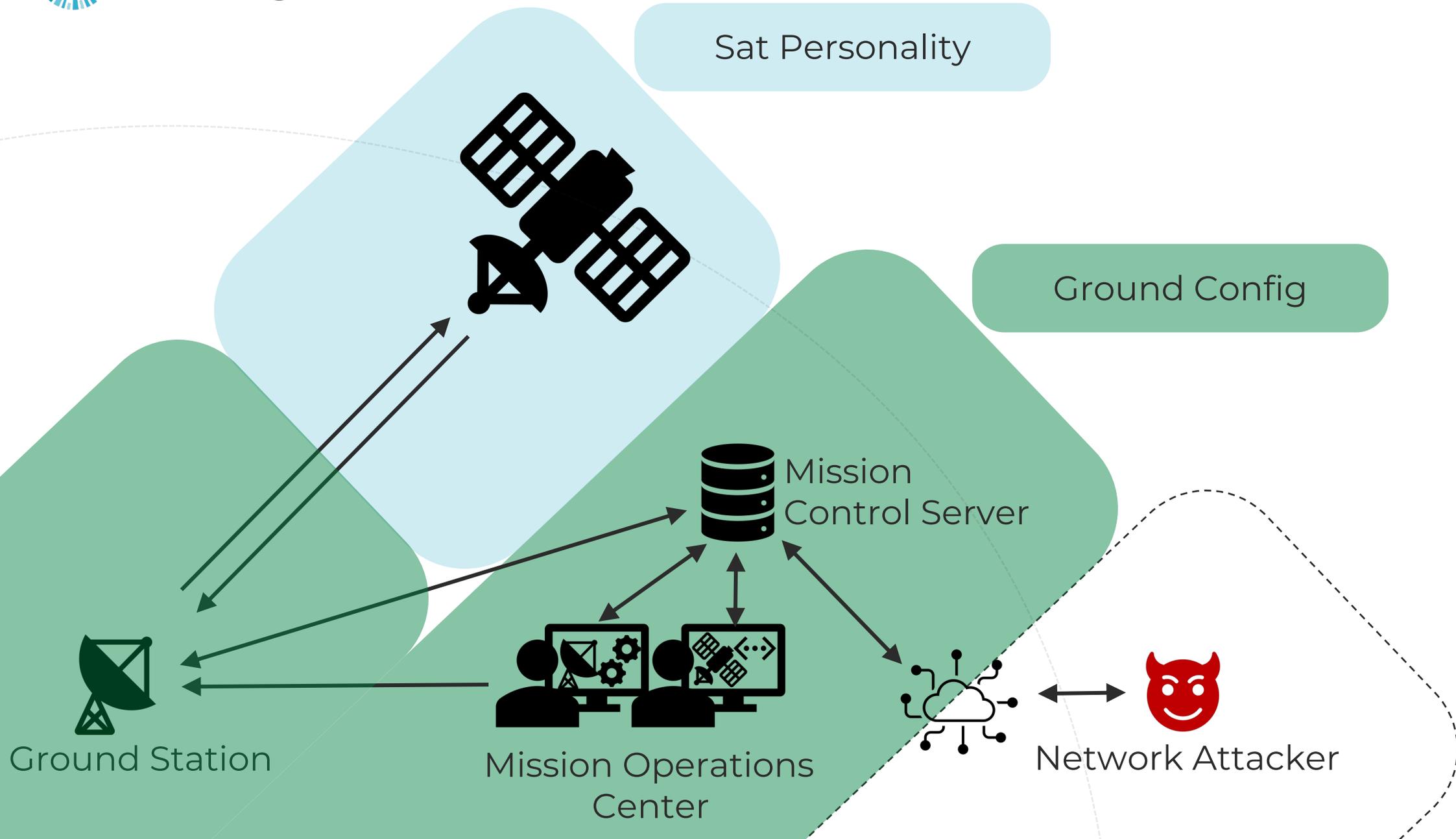


# Delivering Believable Spacecraft





# Configuration





# Delivering Believable Ground Infrastructure

- Operator **workstation** with Remote Desktop



# Delivering Believable Ground Infrastructure

- Operator **workstation** with Remote Desktop
- Network with **Mission Control Server** and **Ground Station**



# Delivering Believable Ground Infrastructure

- Operator **workstation** with Remote Desktop
- Network with **Mission Control Server** and **Ground Station**
- **Mission Control Client**



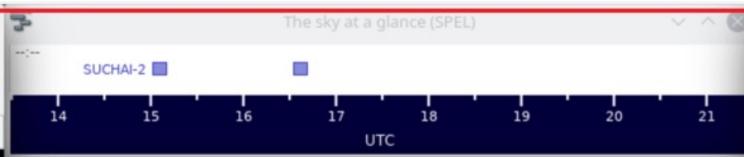
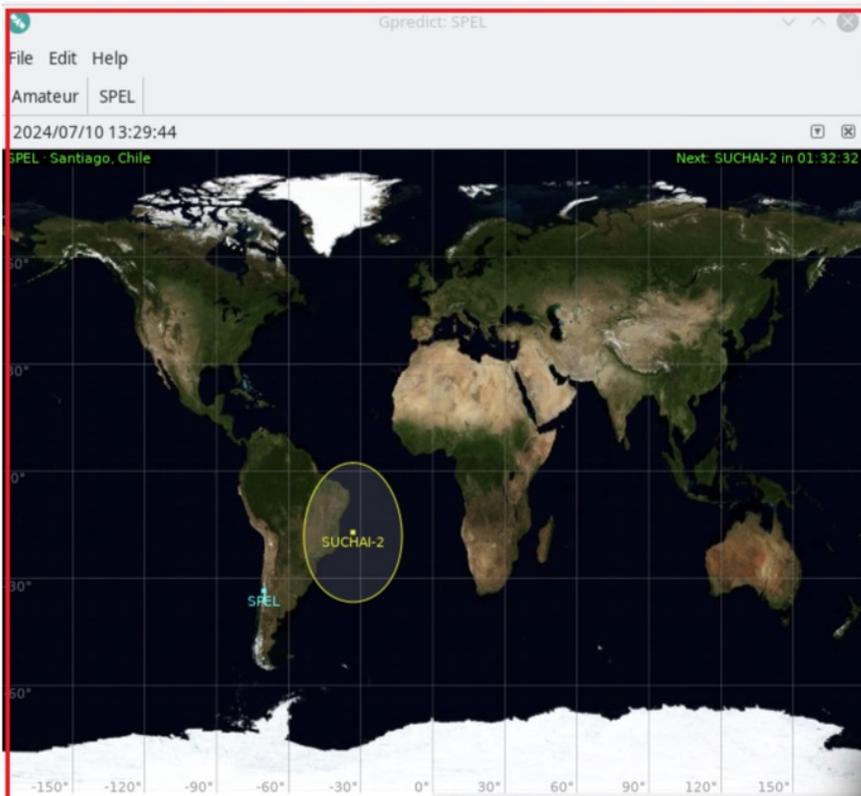
# Delivering Believable Ground Infrastructure

- Operator **workstation** with Remote Desktop
- Network with **Mission Control Server** and **Ground Station**
- **Mission Control Client**
- **Ground Station Control Software**



# Delivering Believable Ground Infrastructure

- Operator **workstation** with Remote Desktop
- Network with **Mission Control Server** and **Ground Station**
- **Mission Control Client**
- **Ground Station Control Software**
- **Standard** Operational **tools** bundled for Realism



Gpredict Radio Control: SPEL

**Downlink**

▲▲▲▲▲▲▲▲▲▲

4 3 7 . 2 3 0 . 0 0 0 Hz

▼▼▼▼▼▼▼▼▼▼

Doppler: 7185 Hz      LO: 0 MHz

**Radio: 145.890.000 Hz**

**Uplink**

▲▲▲▲▲▲▲▲▲▲

4 3 7 . 2 5 0 . 0 0 0 Hz

▼▼▼▼▼▼▼▼▼▼

Doppler: -7185 Hz      LO: 0 MHz

**Radio: 145.890.000 Hz**

Target: SUCHAI-2 [Track] [T] [L]

Az: 73.73° Range: 4159 km  
El: -13.31° Rate: -4.926 km/s

Settings: 1. Device: SPEL-GS [Engage] 2. Device: None Cycle: 1000 msec

**AOS in 01:32:29**

Upcoming passes for SUCHAI-2

AOS	LOS	Duration	Max El	AOS Az	LOS Az
2024/07/10 15:02:14	2024/07/10 15:11:14	00:09:00	18.01°	42.75°	172.55°
2024/07/10 16:33:49	2024/07/10 16:42:20	00:08:30	12.79°	333.85°	215.31°
2024/07/11 03:48:50	2024/07/11 03:58:19	00:09:29	23.55°	154.10°	11.77°

[Print] [Save] [Close]

Gpredict Rotator Control: SPEL

**Azimuth**

▲▲▲▲▲

4 2 . 7 5 °

▼▼▼▼▼

Read: ---

**Elevation**

▲▲▲▲▲

0 . 0 0 °

▼▼▼▼▼

Read: ---

Target: SUCHAI-2 [Track]

Az: 73.73°  
El: -13.31°  
ΔT: 01:32:29

Settings: Device: SPEL-GS [Engage] [Monitor] Cycle: 1000 msec Tolerance: 3.00 deg

SPEL

Next: SUCHAI-2 in 01:32:29

Two circular diagrams. The left one shows concentric circles representing signal strength or range. The right one shows concentric circles with a blue arc indicating the satellite's path across the sky, with time markers: 15:00, 15:04, 15:05, 15:07, 15:09.

**SUCHAI-2**

- Azimuth : 73.73°
- Elevation : -13.31°
- Slant Range : 4159 km
- Range Rate : -4.926 km/sec
- Next Event : AOS: 2024/07/10 15:02:14
- SSP Loc. : HH32
- Footprint : 4335
- Altitude : 387 km
- Velocity : 7.679
- Doppler@100M : 1643
- Sig. Loss : 144.7
- Sig. Delay : 13.87
- Mean Anom. : 7.17°
- Orbit Phase : 10.08
- Orbit Num. : 12733
- Visibility : Daylight

Serial Commander

Archivo Herramientas Ayuda

Conexión

IP: 172.17.58.76  
Puerto: 8001  
[Abrir] [Cerrar]

Opciones

Agregar marca de tiempo  
 Auto scroll

Lista de comandos

- trx\_send\_beacon
- trx\_read\_reg <registro>
- trx\_tm <funcion>
- trx\_getstatustrx\_set\_beacon [<text>]
- trx\_set\_mode <mode>
- trx\_set\_tm\_pwr <pwr>
- trx\_set\_bc\_pwr <pwr>
- trx\_read\_tc\_frame

[Eco]  LF  CR [Enviar]

~ : telnet — Konsole

```

log_set %d %d %d
fp_set_cmd %d %d %d %d %d %d %d %d %s %n
fp_set_cmd_unix %d %d %d %s %n
fp_set_cmd_dt %d %d %d %s %n
fp_del_cmd %d %d %d %d %d %d
fp_del_cmd_unix %d %d %d %d %d %d
fp_show
fp_reset
fp_purge
com_ping %d
com_send_rpt %d %s
com_send_cmd %d %n
com_send_tc %d %n
com_send_data %d %d %n
com_debug
com_set_time_node %d
tm_parse_status
tm_parse_string
tm_send_status %d
tm_send_var %d %s
tm_get_last %u
tm_get_single %u %u
tm_send_last %u %u
tm_send_all %u %u
tm_send_n %u %u %u
tm_parse_payload %
tm_set_ack %u %u
tm_send_cmds %d
tm_send_fp %d
tm_print_fp
tm_dump %d %s
tm_send_file %s %d
tm_parse_file
tm_send_file_part %s %d %d %d %d %d
tm_merge_file %s %d
tm_ls %s %d
obc_get_sensors
obc_update_status
obc_set_mode %s
obc_cancel_deploy
tm_send_msg %d %n
tm_parse_msg
tm_send_beacon %d
tm_parse_beacon
tle_send %d %s

```

[IN 0][1720618158][Executer] Command result: 1



# Evaluation

- **10 experienced** SmallSat **operators** (1–10 years; 1–5 missions; diverse regions/sectors)
- **Overall realism:** 90% agreed they “would not be able to distinguish” HoneySat from the real mission.
- We support interactions for **33 / 38 SPACE-SHIELD techniques**



# Point of Entry

- Website with **weak credentials** as initial **entry point**
- **Multiple entry styles** tested:
  1. Web-based mission control interface
  2. Ground-station appliance config page
  3. Internal “mission” website
- **Best-performing lure**: a Django based mission-style website with documentation + remote-desktop credentials to entice access



# Deployments

<b>Deployment</b>	<b>Sat. Personality</b>	<b>Real Mission Owner</b>	<b>HoneySat Region</b>	<b>Duration (months)</b>
Cloud	PIXL-1	DLR	Germany	6
Cloud	PIXL-1	DLR	Germany	6
Cloud	ACS3	NASA	USA	6
Cloud	ACS3	NASA	USA	6
On-prem	SUCHAI-2	SPEL	University of Chile	12



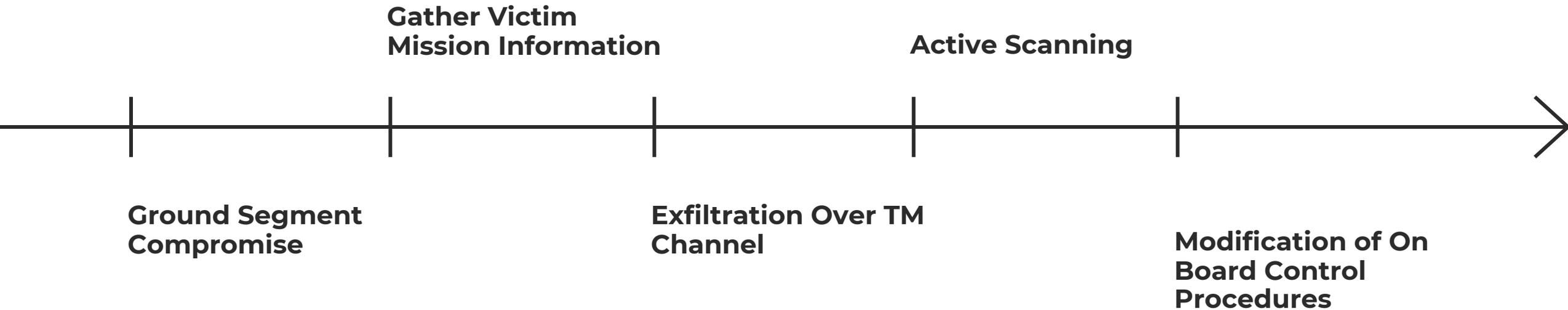
# Interactions

<b>Date</b>	<b>Mission</b>	<b>HoneySat Region</b>	<b>Attacker Geo IP</b>
Jan 18, 2025	ACS3	USA	Egypt
Jan 24, 2025	PIXL-1	Germany	Tor
Jan 24, 2025	ACS3	USA	Tor
Apr 3, 2025	ACS3	USA	USA



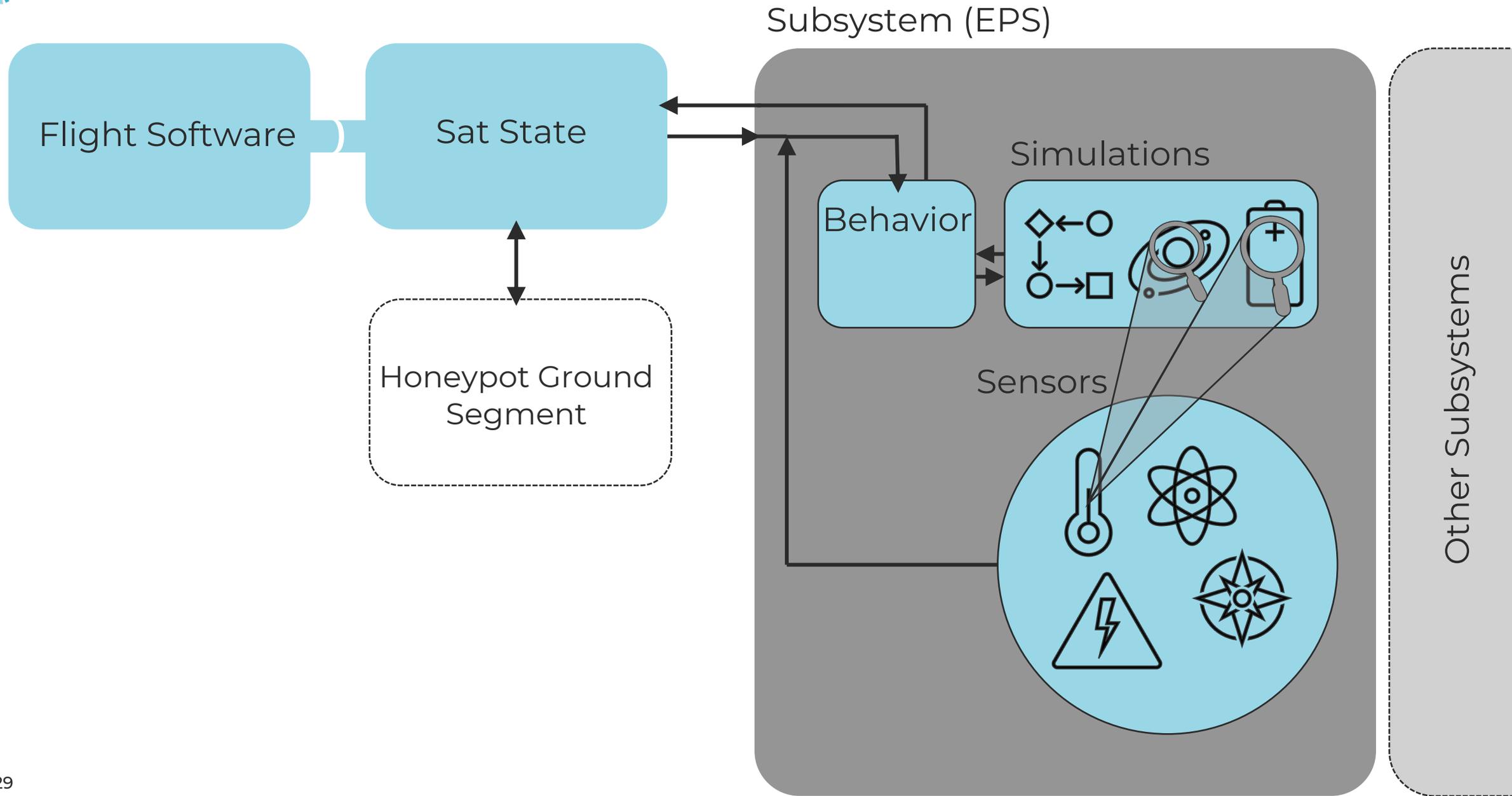
# Attacker Behavior

All Attackers interacting with the MCS Performed **Spacecraft's Components Discovery**



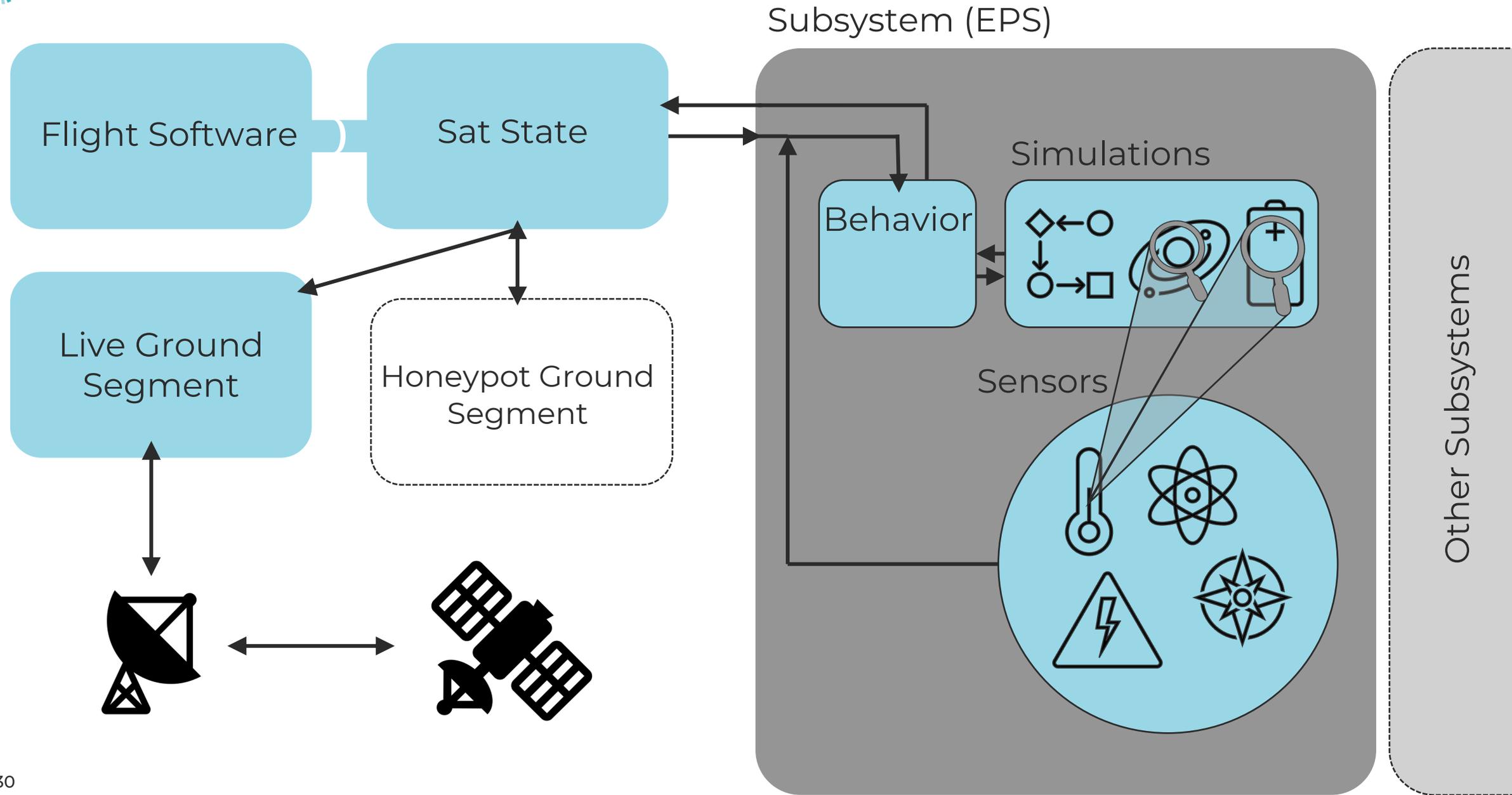


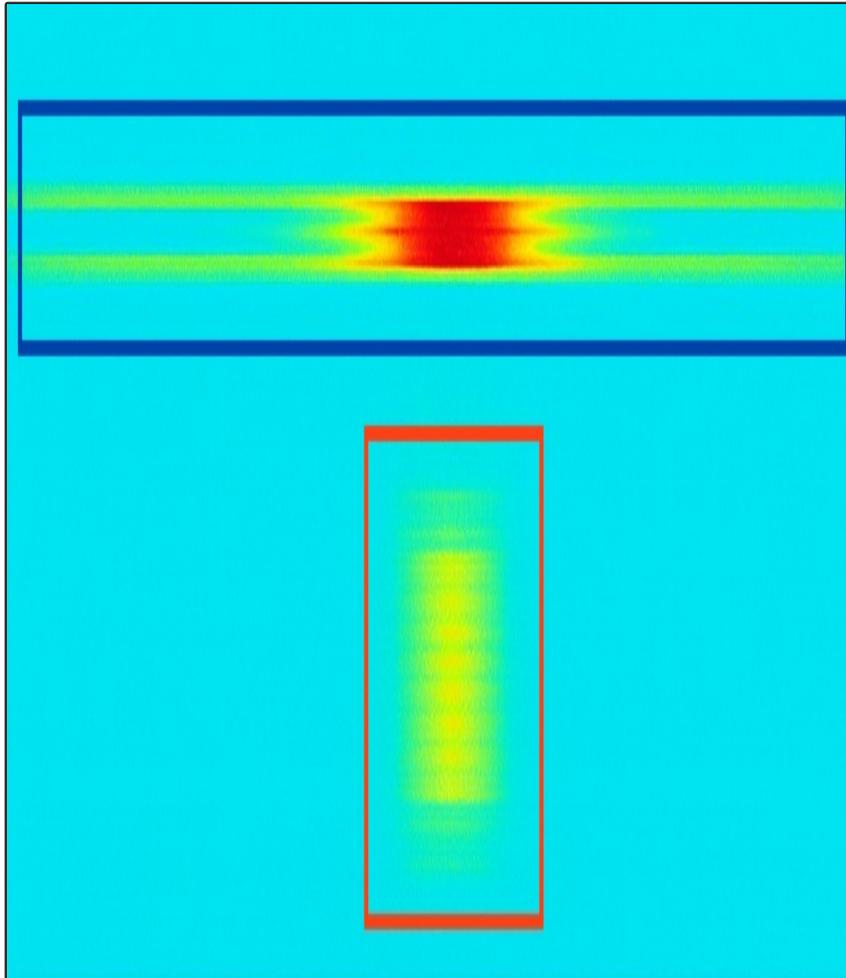
# Delivering Believable Spacecraft





# Delivering ~~Believable~~ Spacecraft





# Satellite In The Loop

*Deceiving attackers observing the real Ground Station*