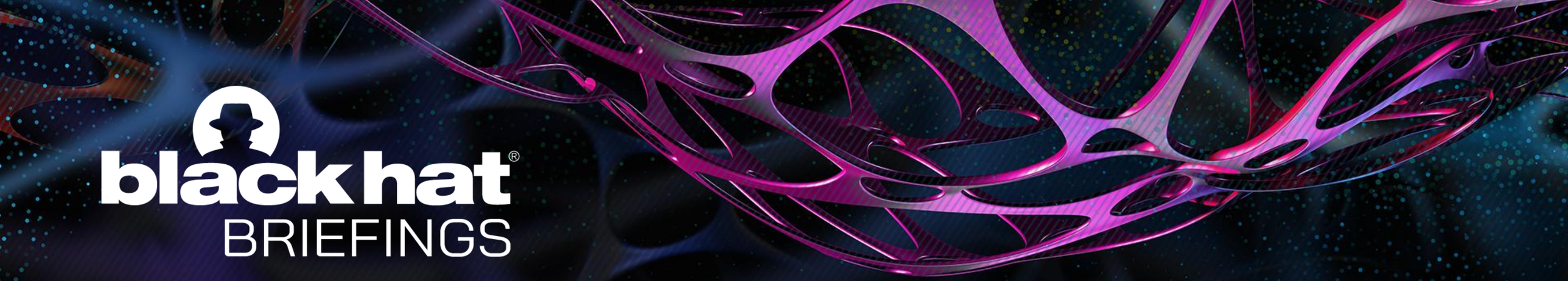


AUGUST 6-7, 2025

MANDALAY BAY / LAS VEGAS

Burning, Trashing, Spacecraft Crashing

A Collection of Vulnerabilities that will End your Space Mission

Andrzej Olchawa, Milenko Starcik, Ricardo Fradique, Ayman Boulaich

VISION SPACE

Andrzej Olchawa

Cybersecurity Engineer

Milenko Starcik

Head of Cybersecurity

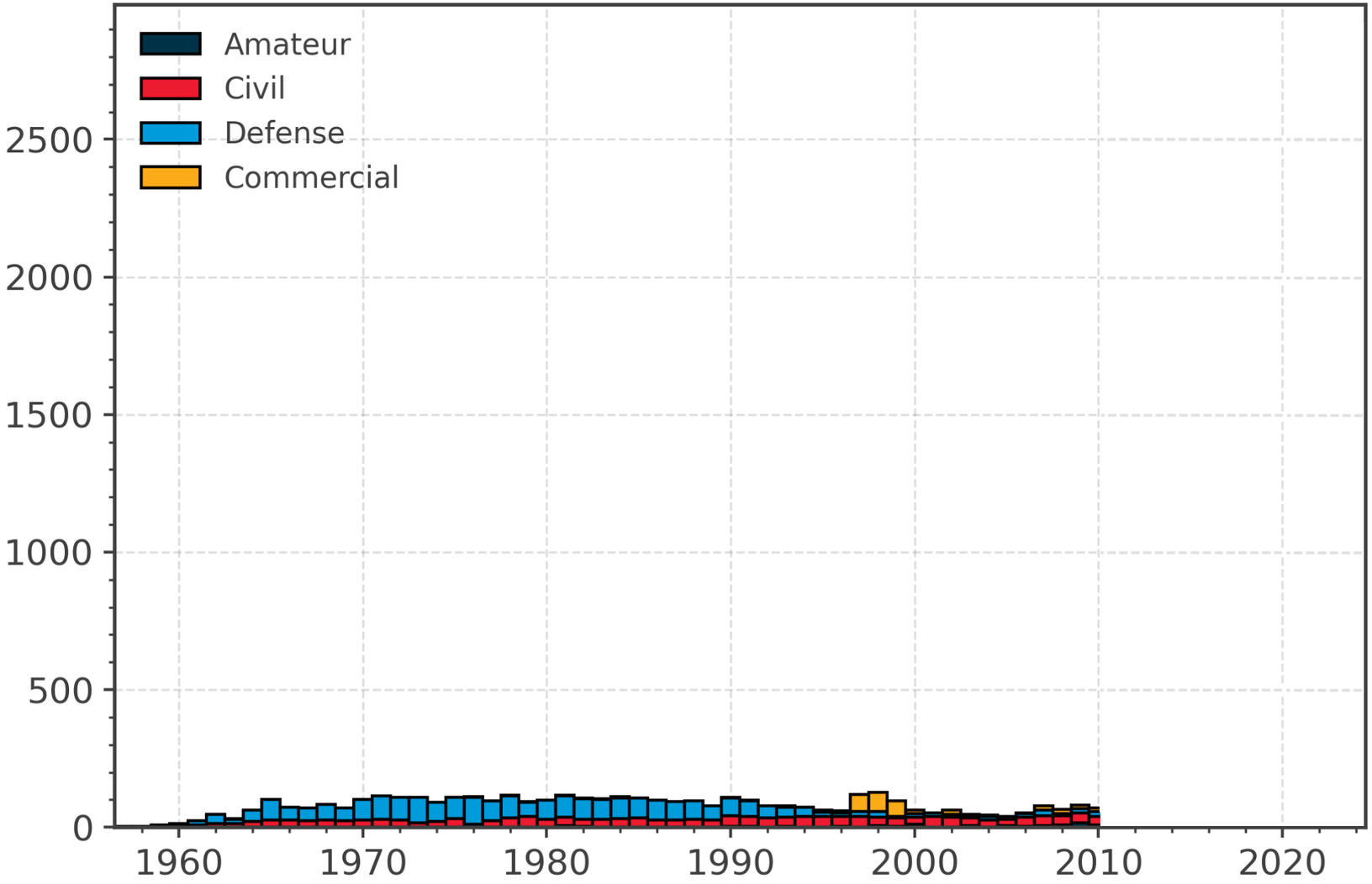
Ricardo Fradique

Cybersecurity Engineer

Ayman Boulaich

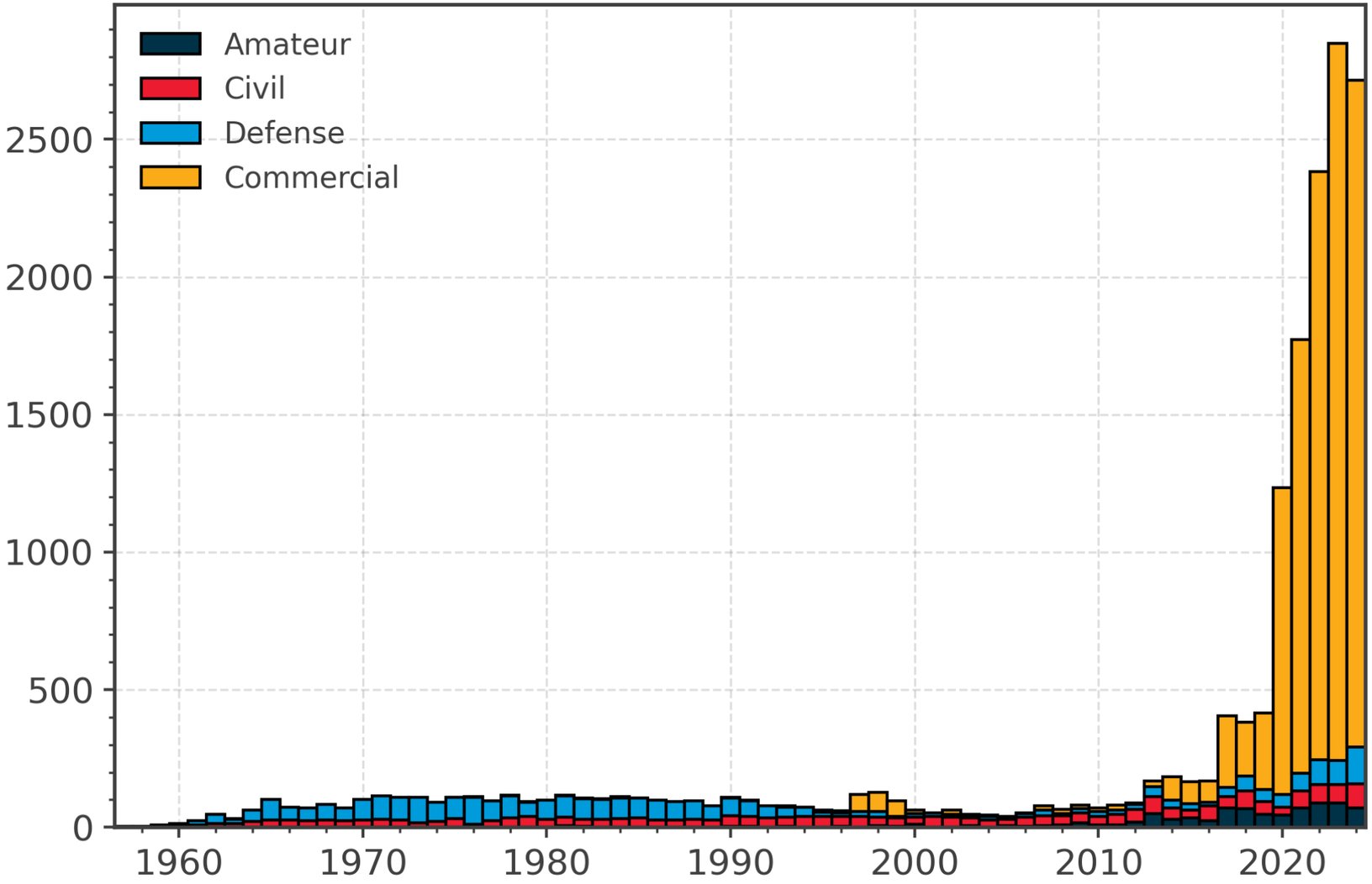
Cybersecurity Intern

Satellites launched to LEO per year



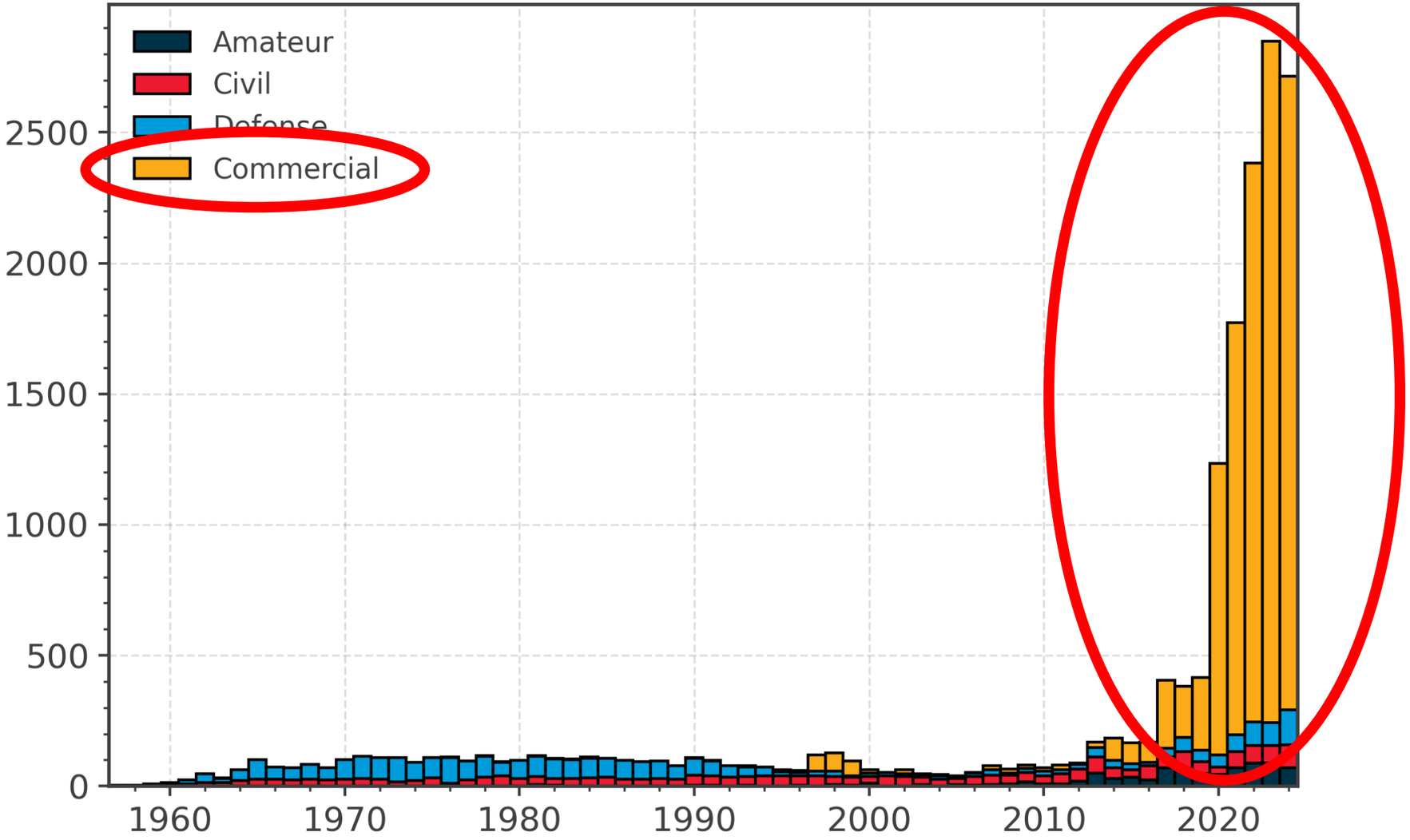
Source: https://sdup.esoc.esa.int/discosweb/statistics/

Constellations



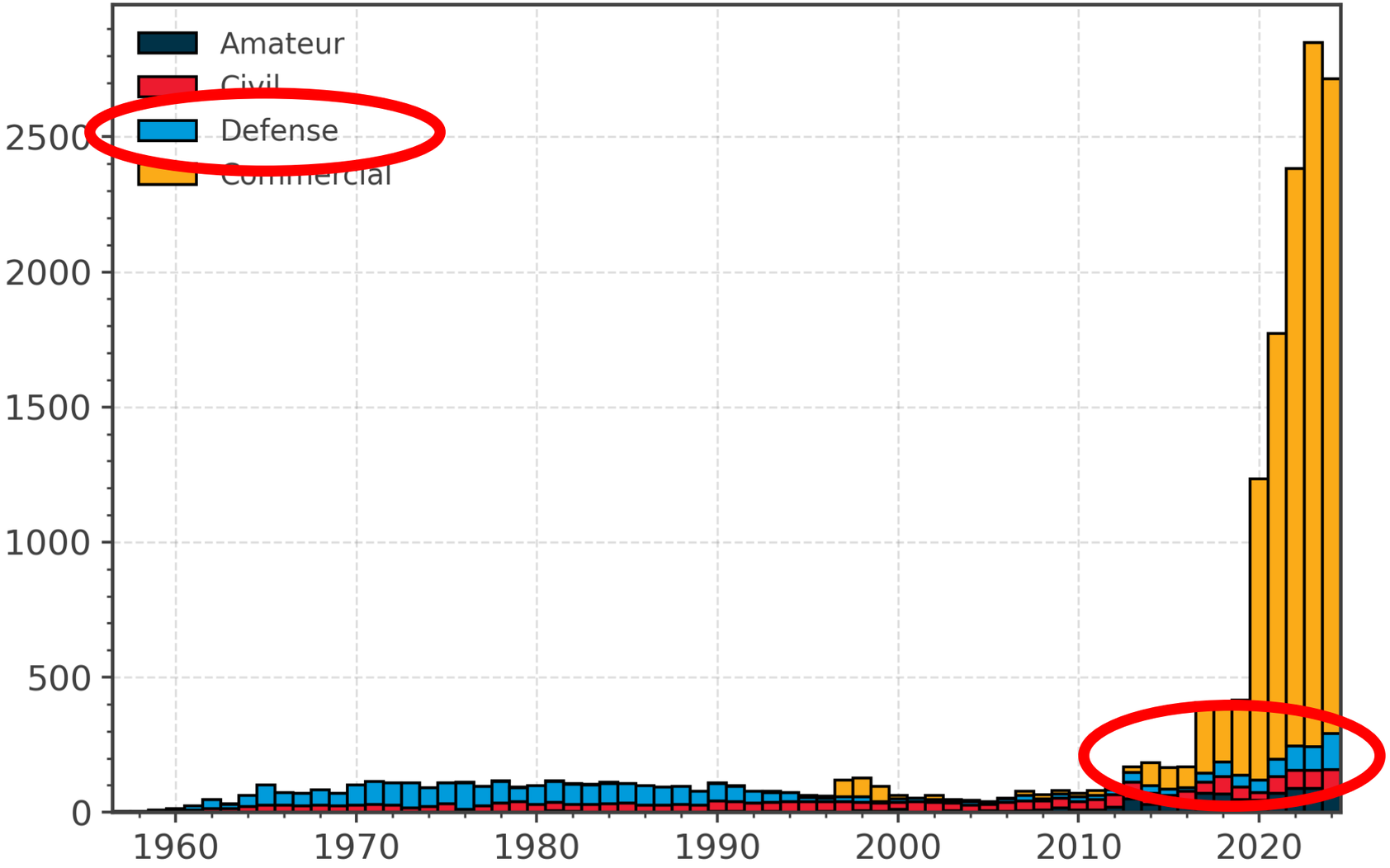
Source: https://sdup.esoc.esa.int/discosweb/statistics/

Commercialization



Source: https://sdup.esoc.esa.int/discosweb/statistics/

Re-Militarization



Source: https://sdup.esoc.esa.int/discosweb/statistics/

Satellite Hacking at Black Hat

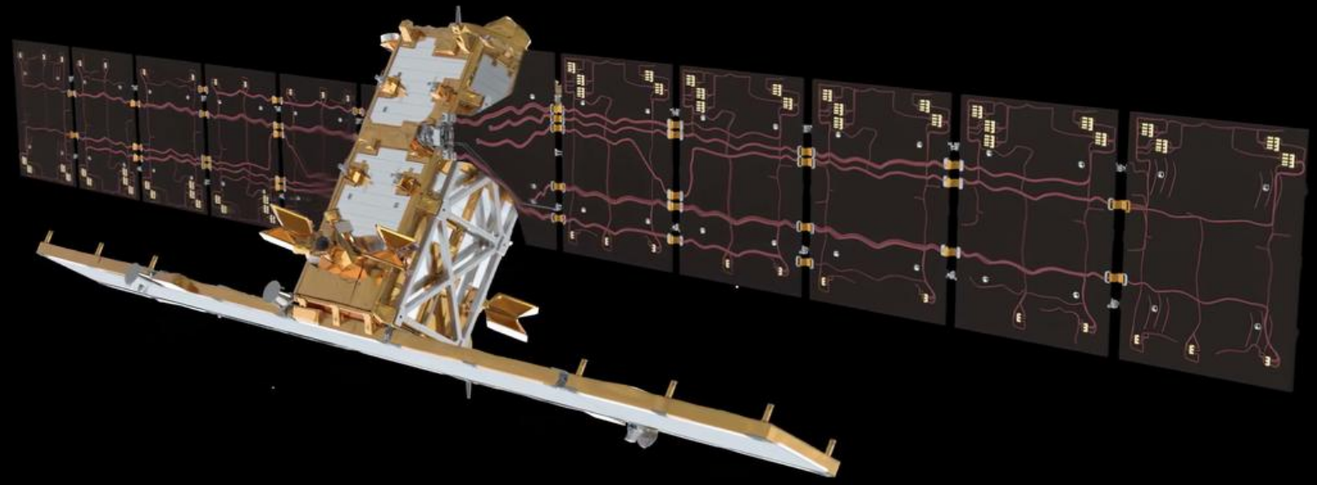
2009

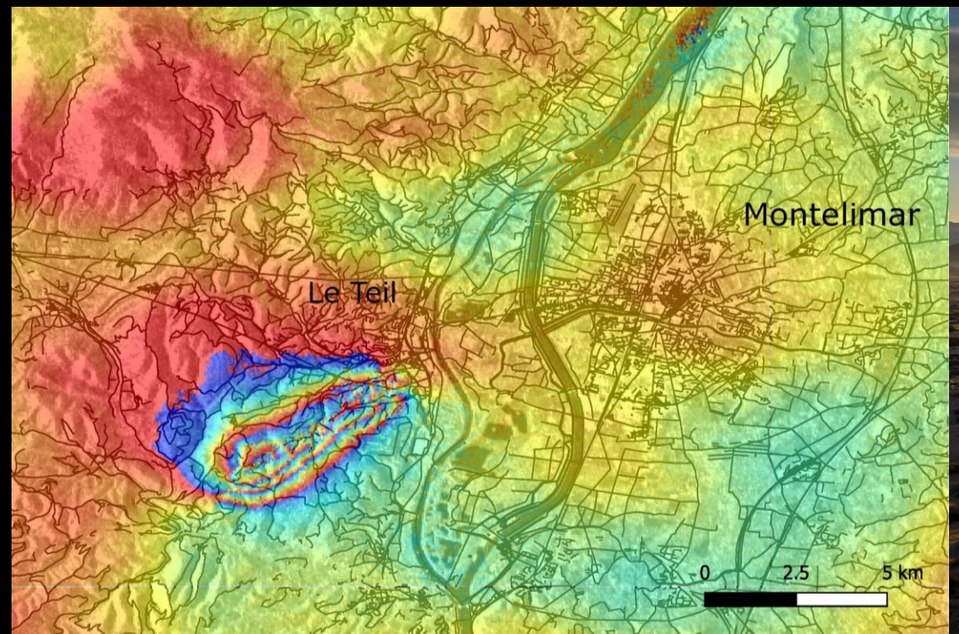
2014

2015

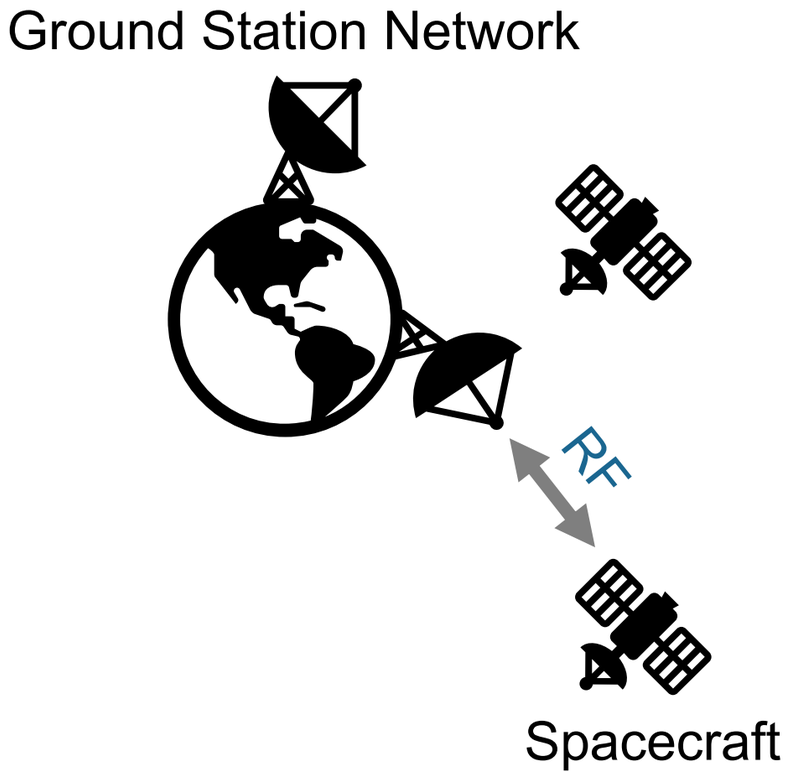
2018 **2022** **2023** **...**

2025?

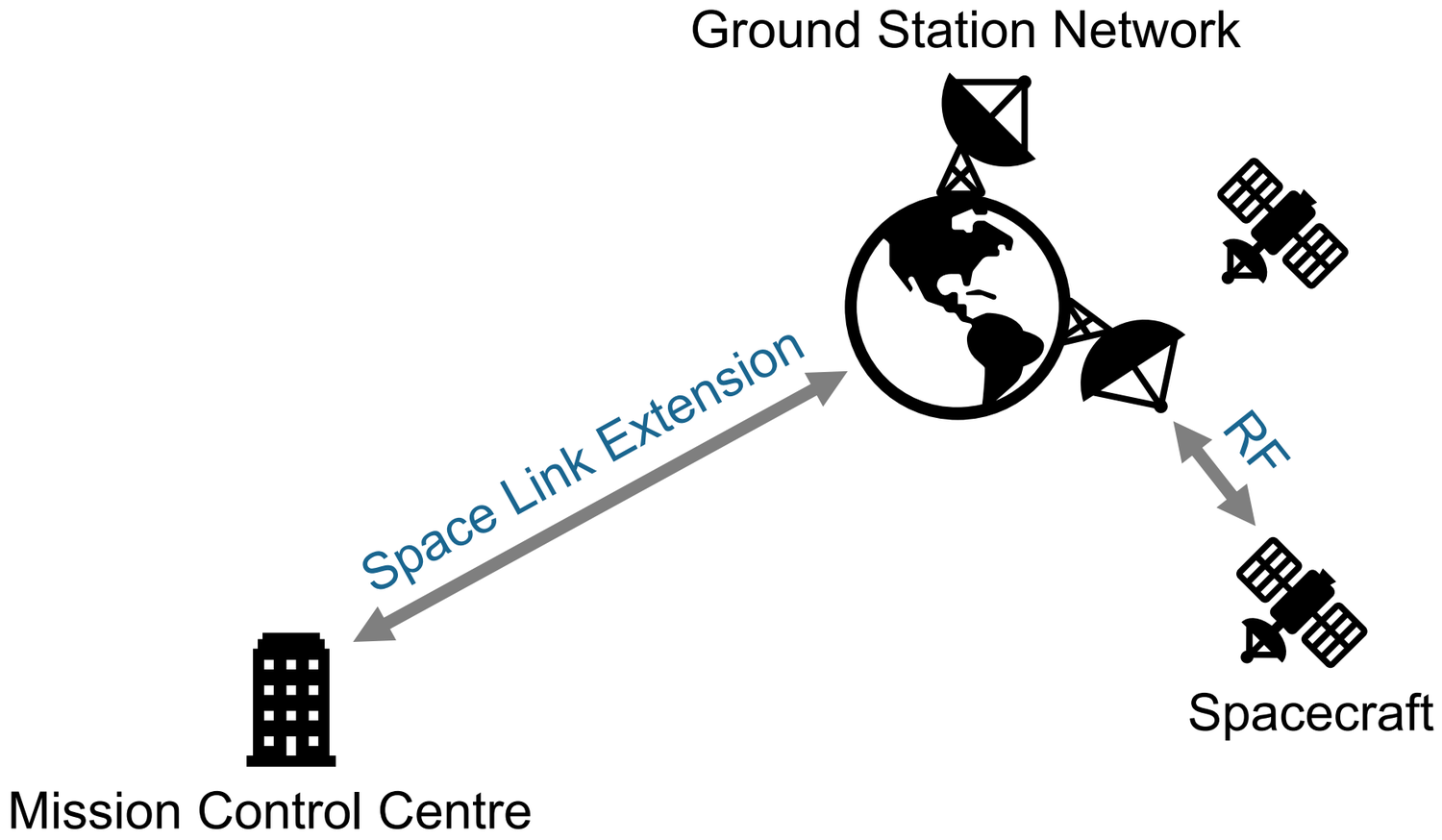



Montelimar
Le Teil
0
2.5
5 km

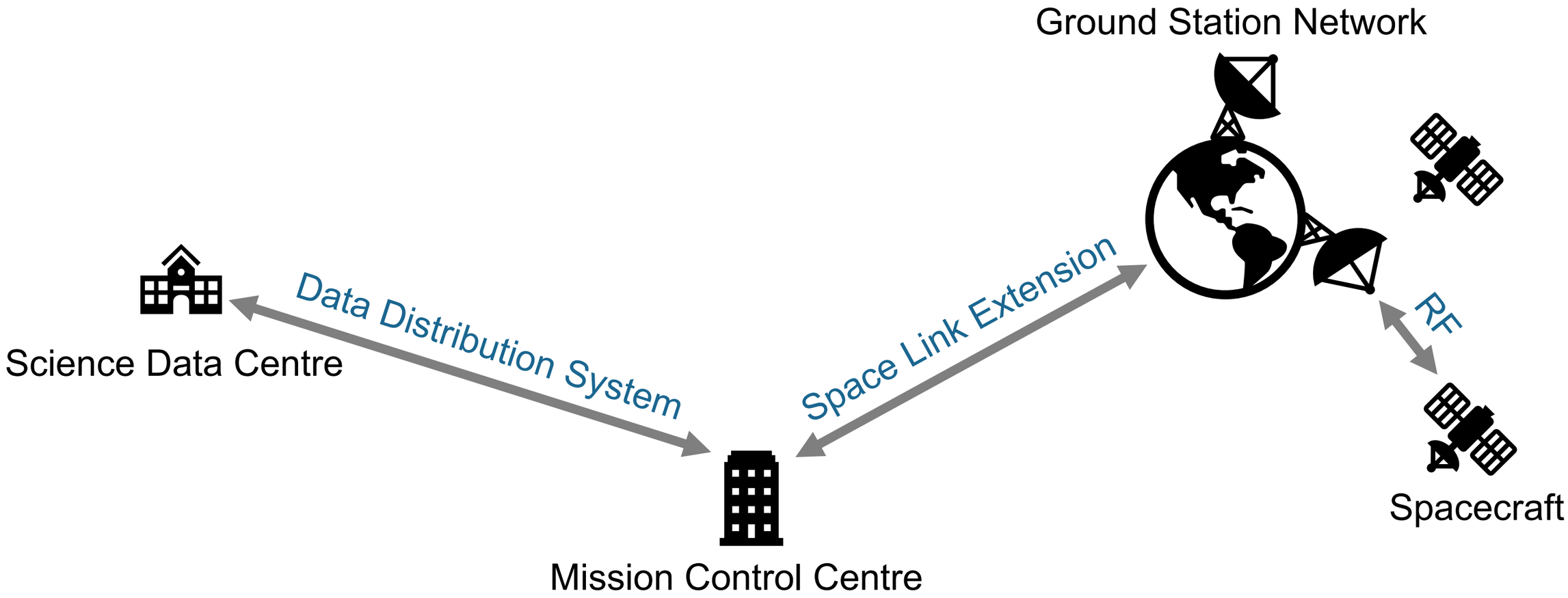
Example Science Mission



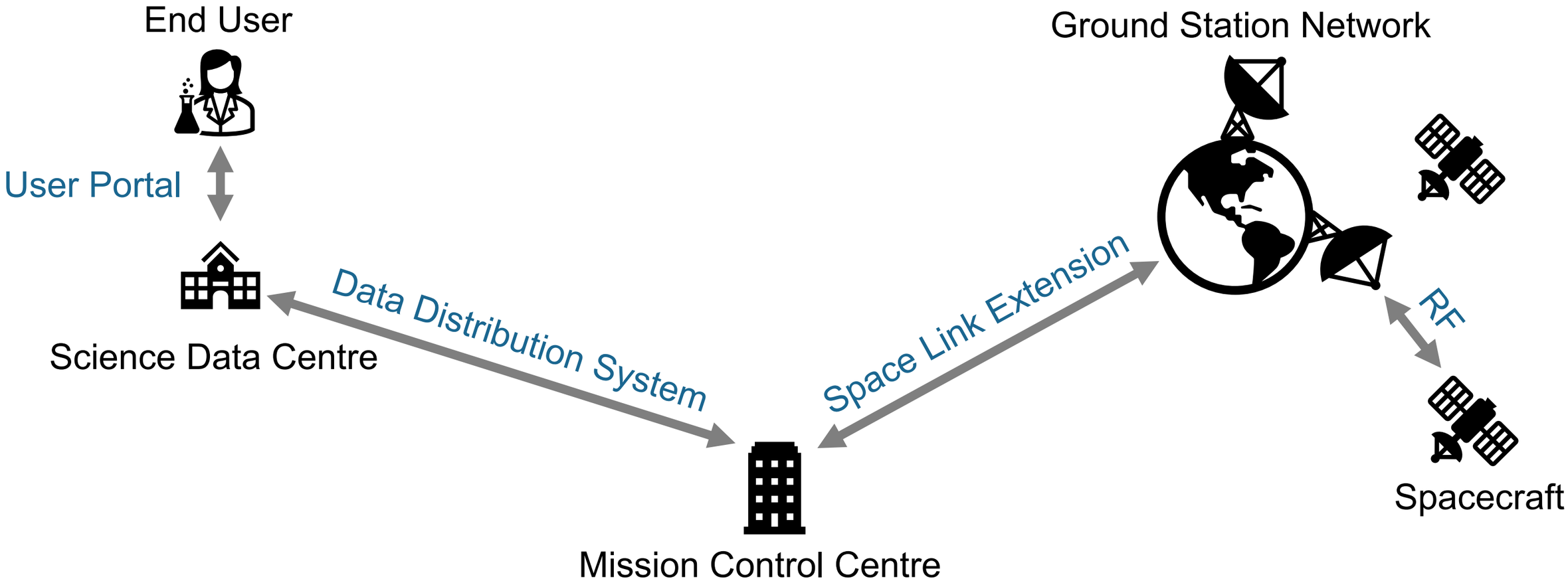
Example Science Mission



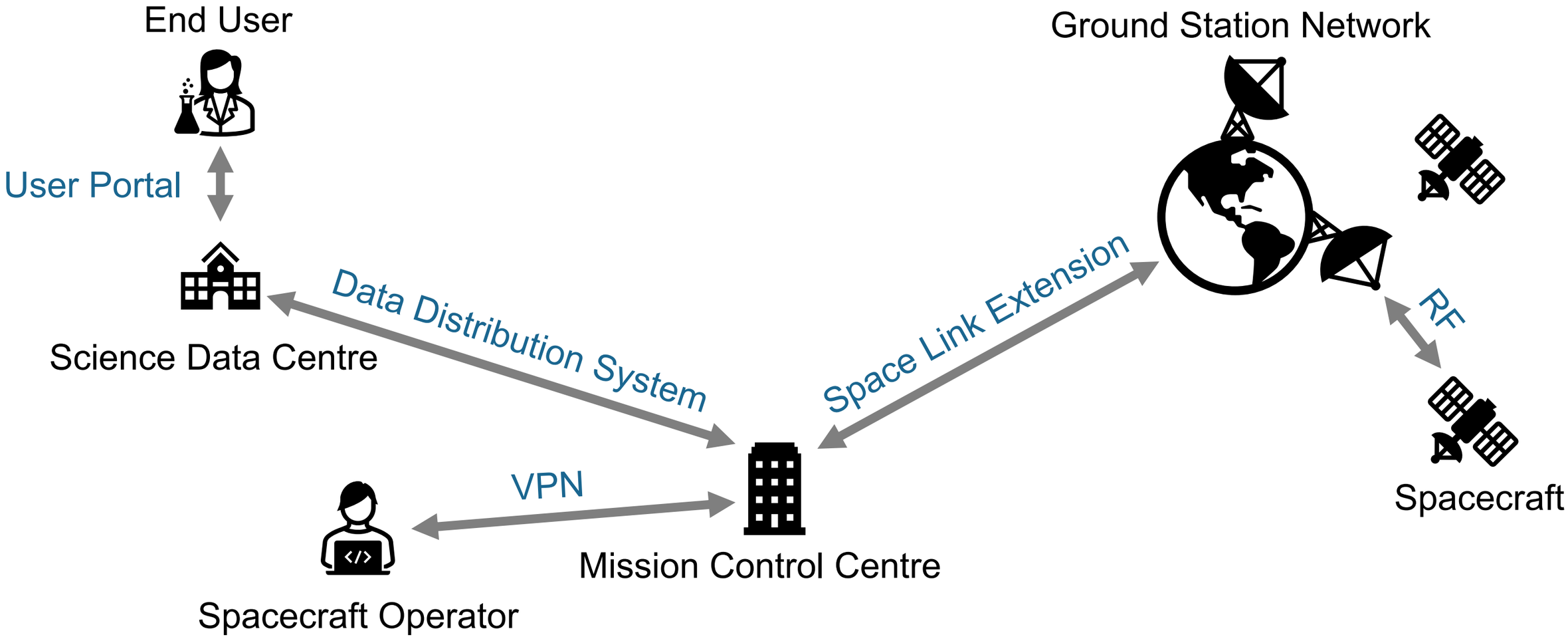
Example Science Mission



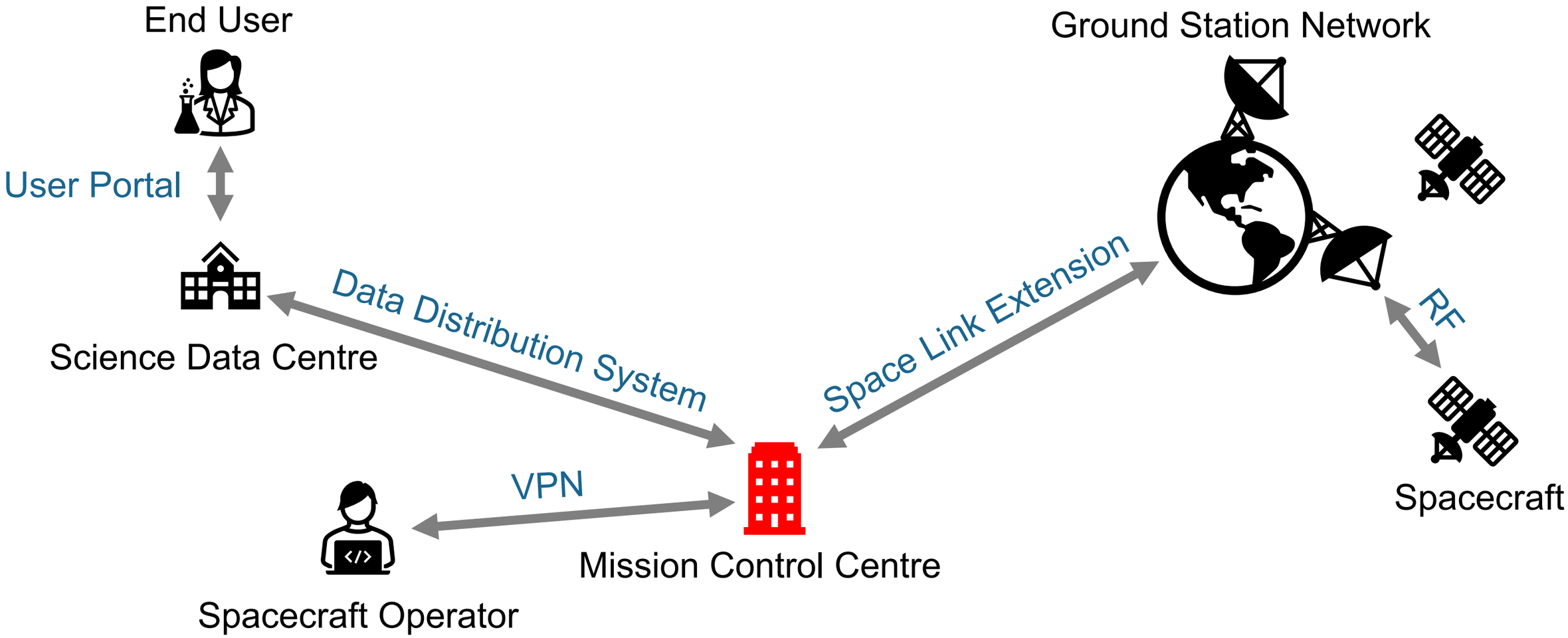
Example Science Mission



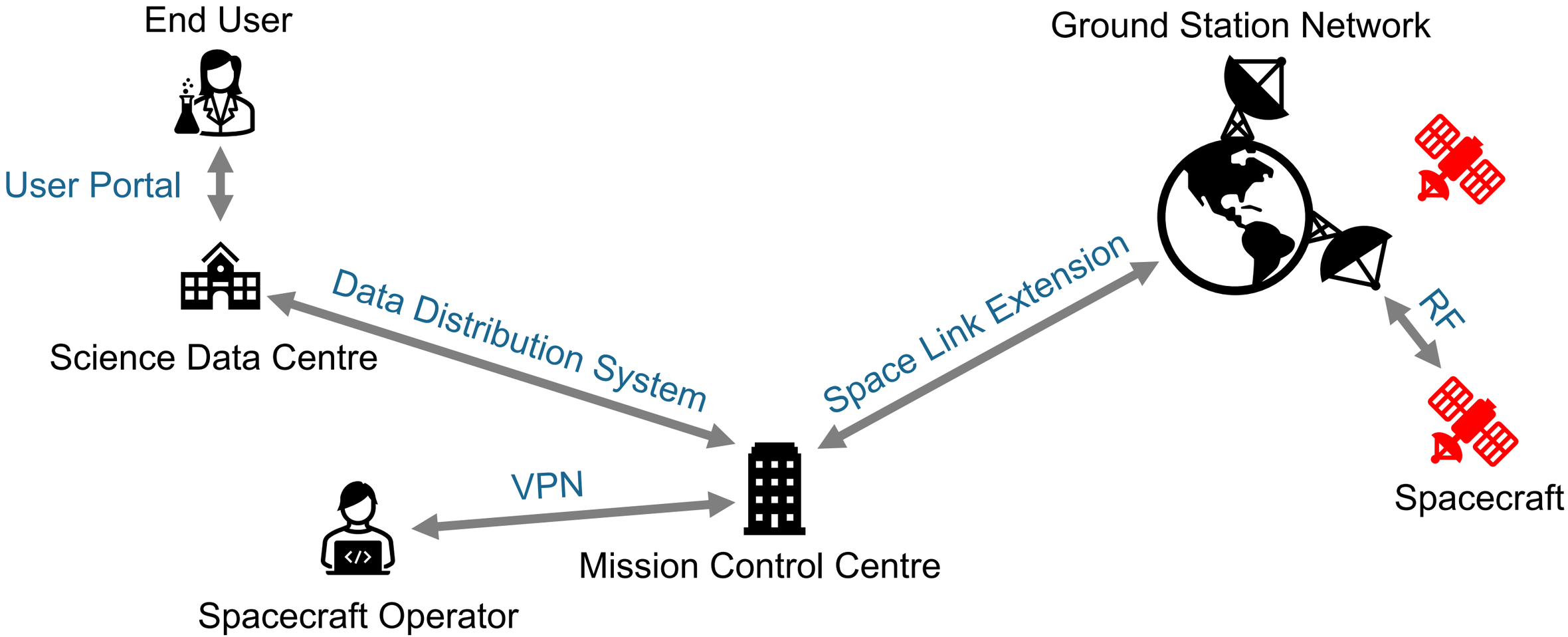
Example Science Mission



Mission Control Software



Onboard Software



Destroying a Satellite

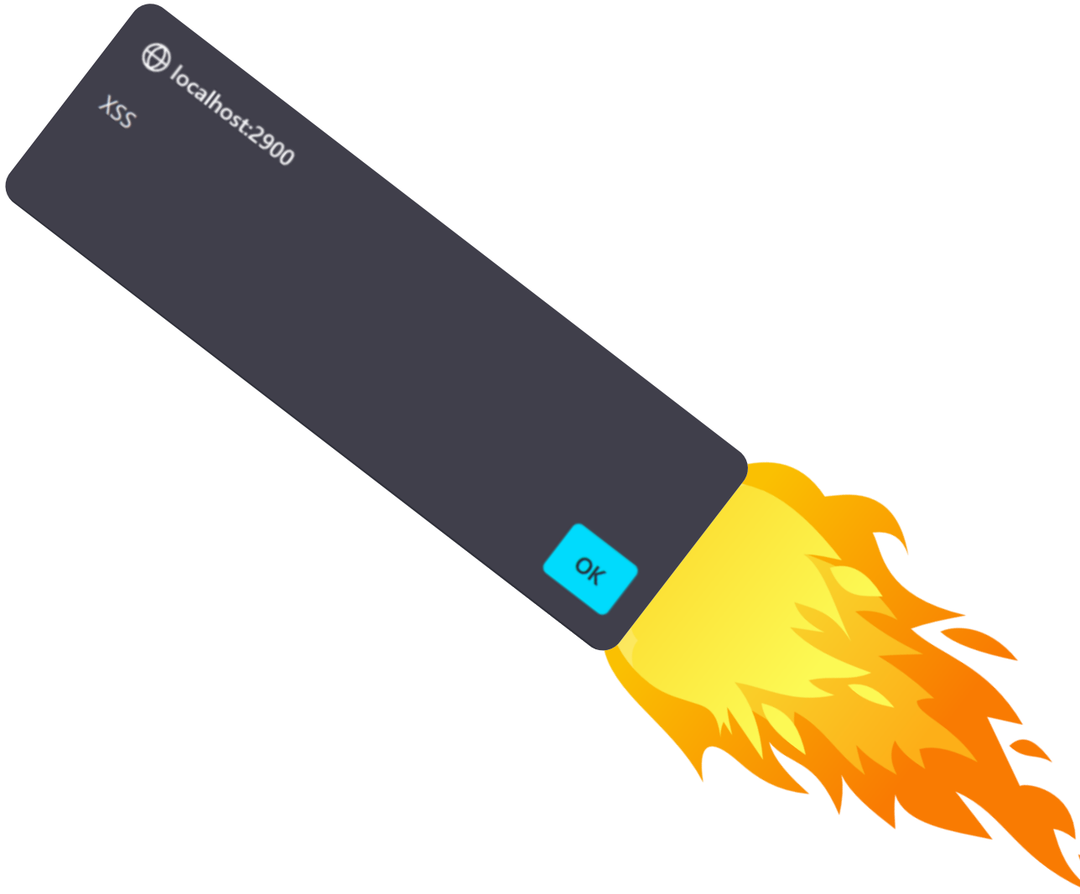
Destroying a Satellite

What you expect

Destroying a Satellite

What you expect

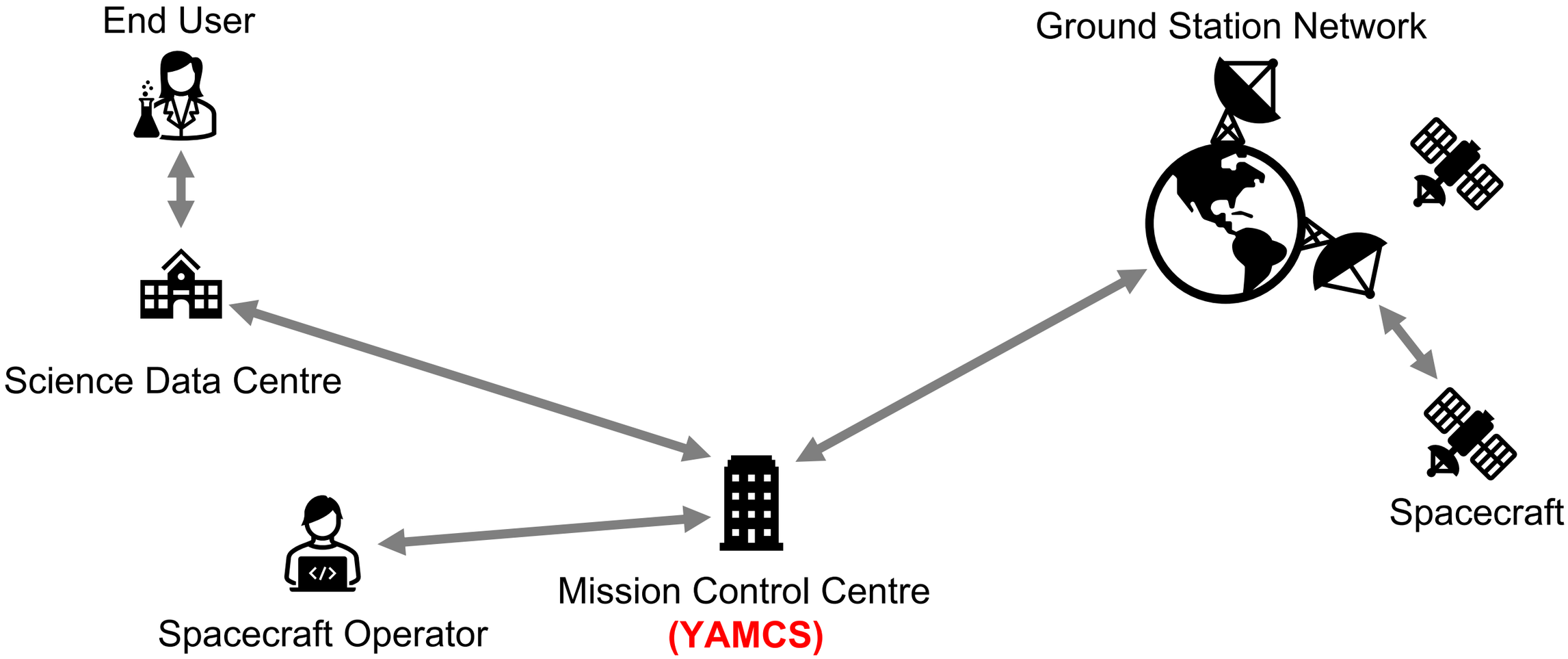
What we found



Water is wet

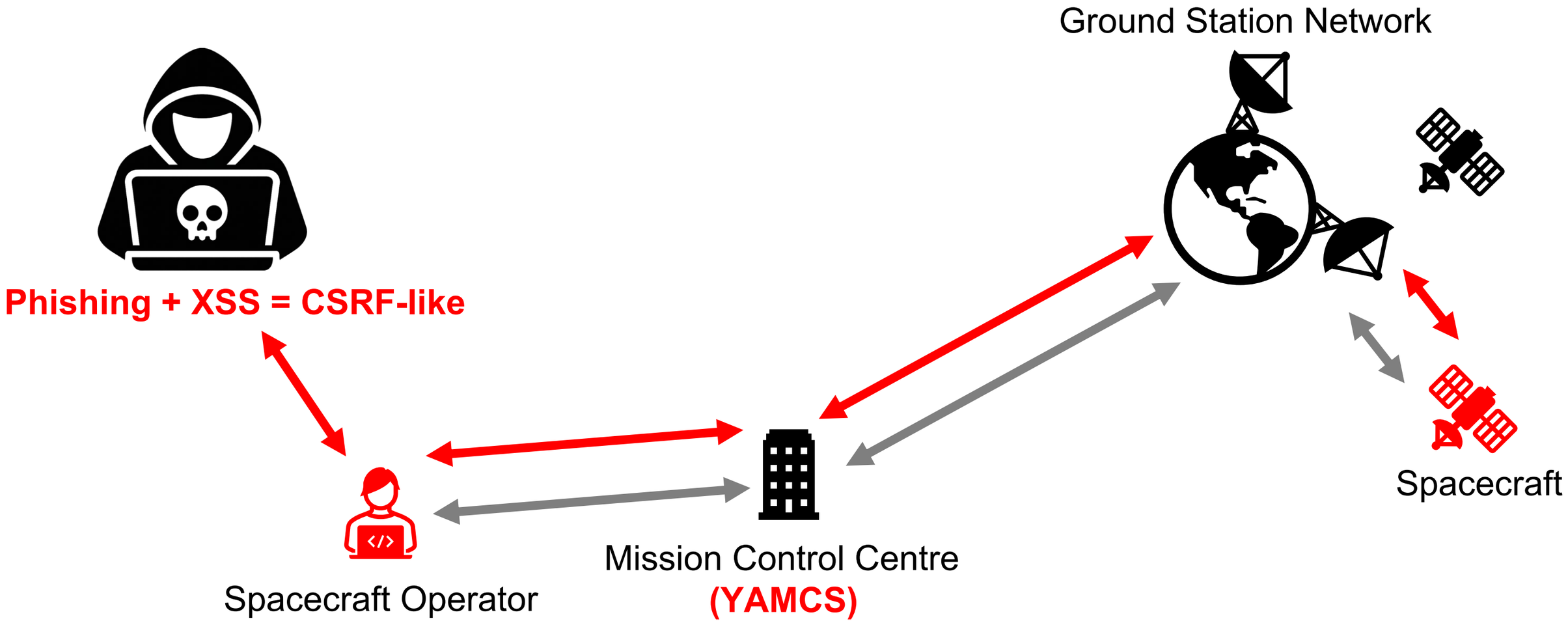
DEMO

YAMCS DEMO



Write-up: https://visionspace.com/yamcs-v5-8-6-vulnerability-assessment/

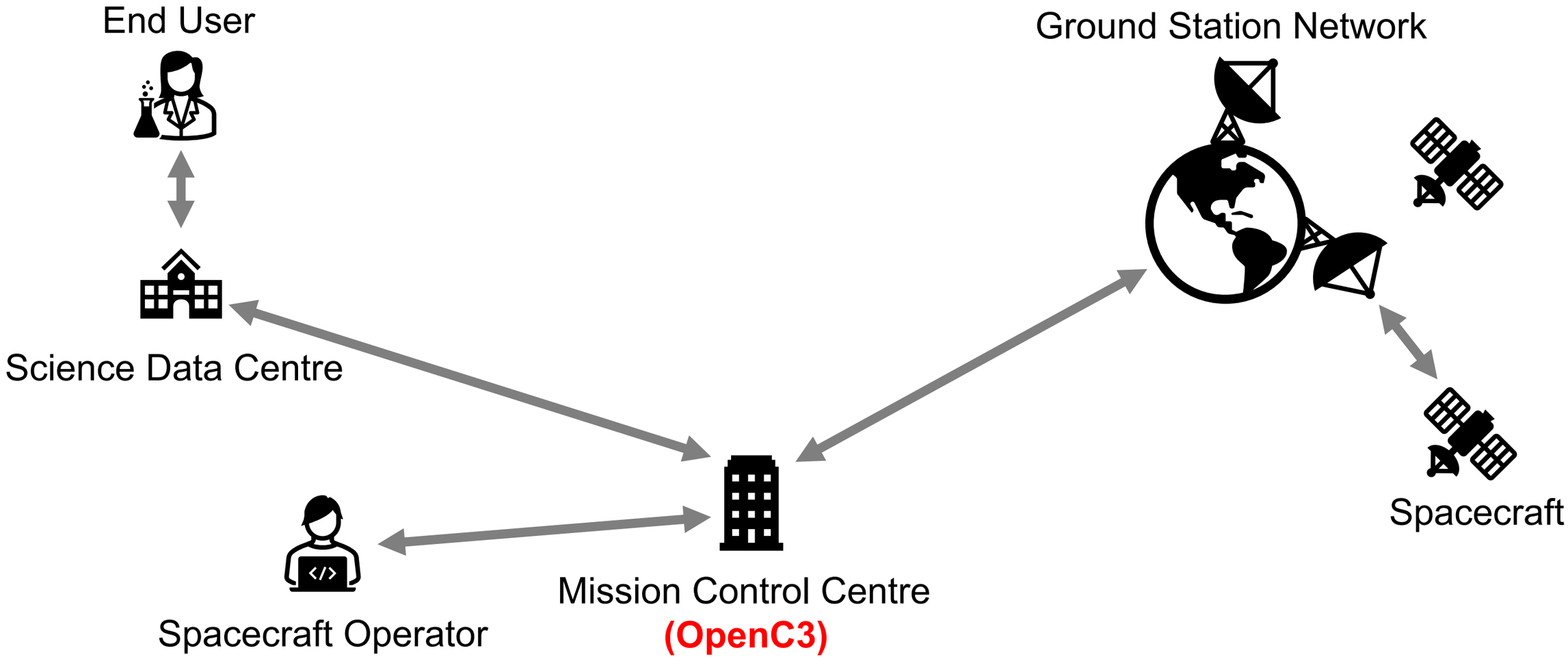
YAMCS DEMO



24 *Write-up: https://visionspace.com/yamcs-v5-8-6-vulnerability-assessment/*

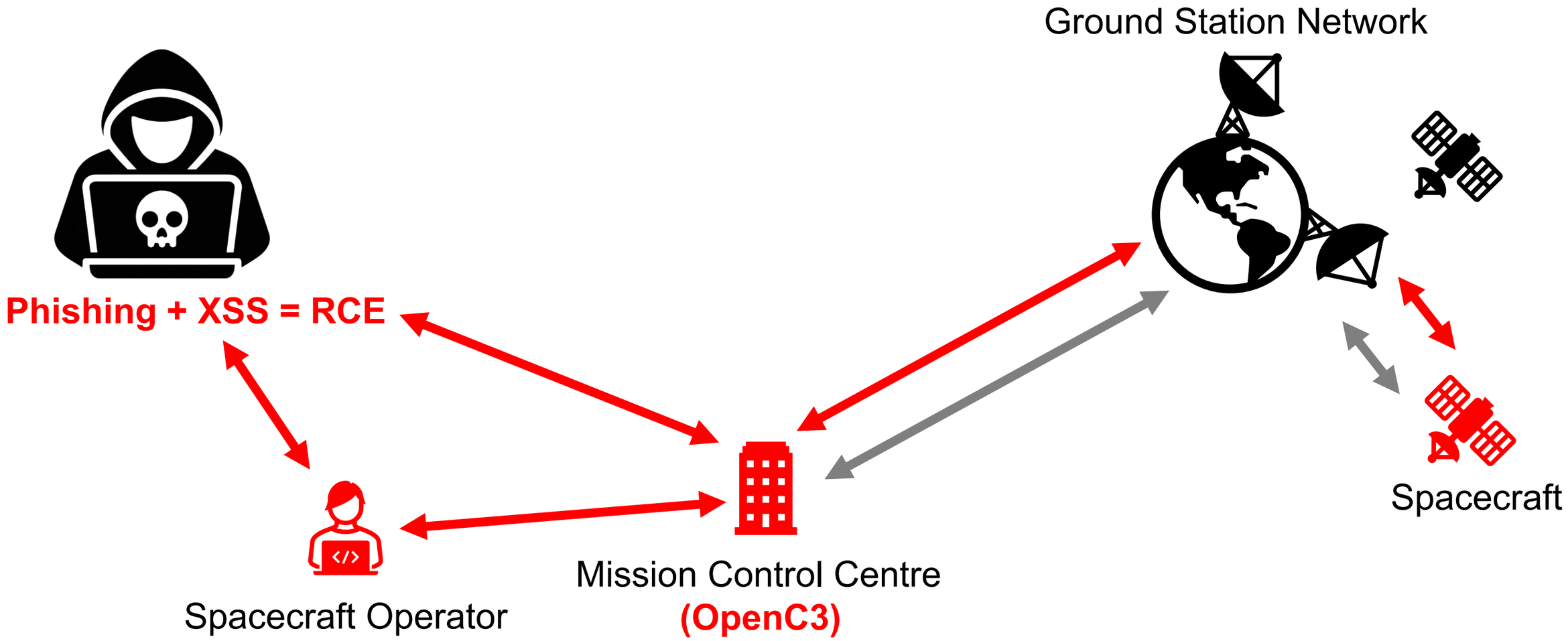
DEMO

OpenC3 DEMO



Write-up: https://visionspace.com/openc3-cosmos-a-security-assessment-of-an-open-source-mission-framework/

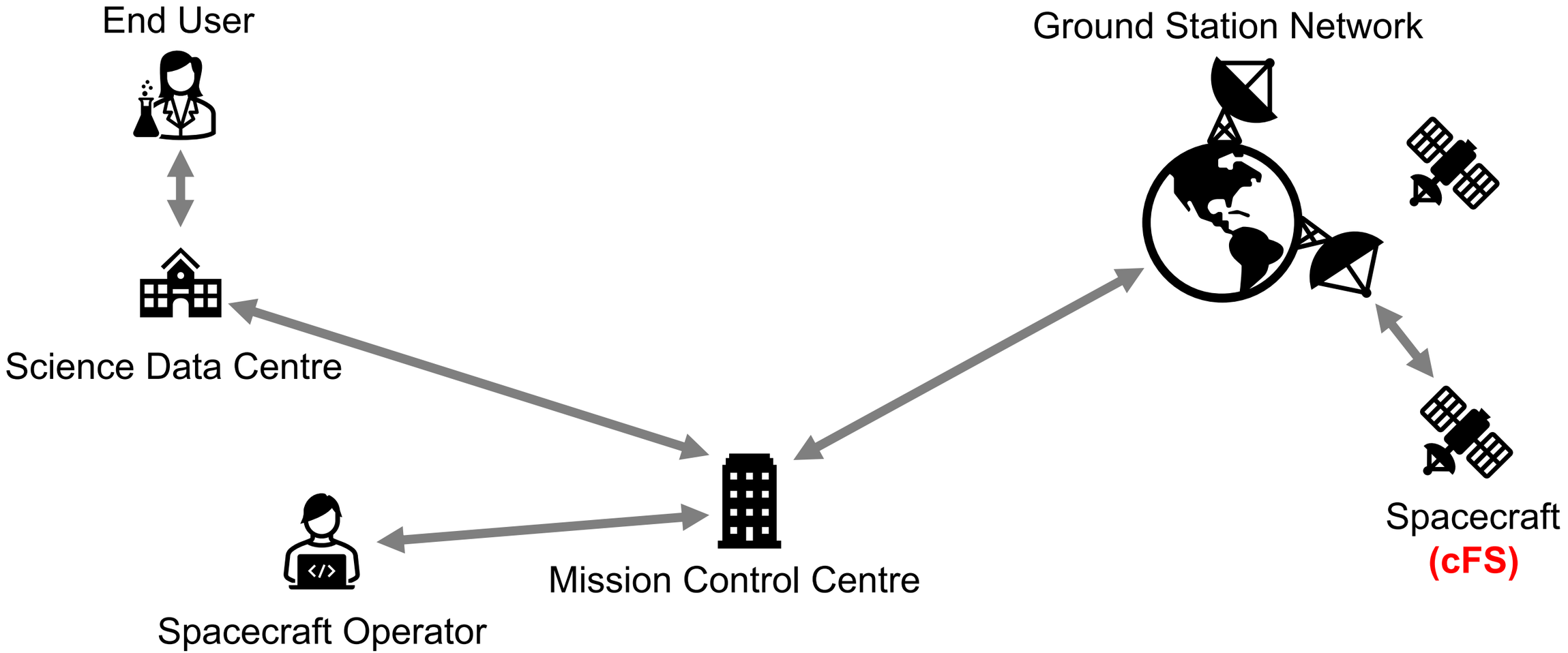
OpenC3 DEMO



 Write-up: https://visionspace.com/openc3-cosmos-a-security-assessment-of-an-open-source-mission-framework/

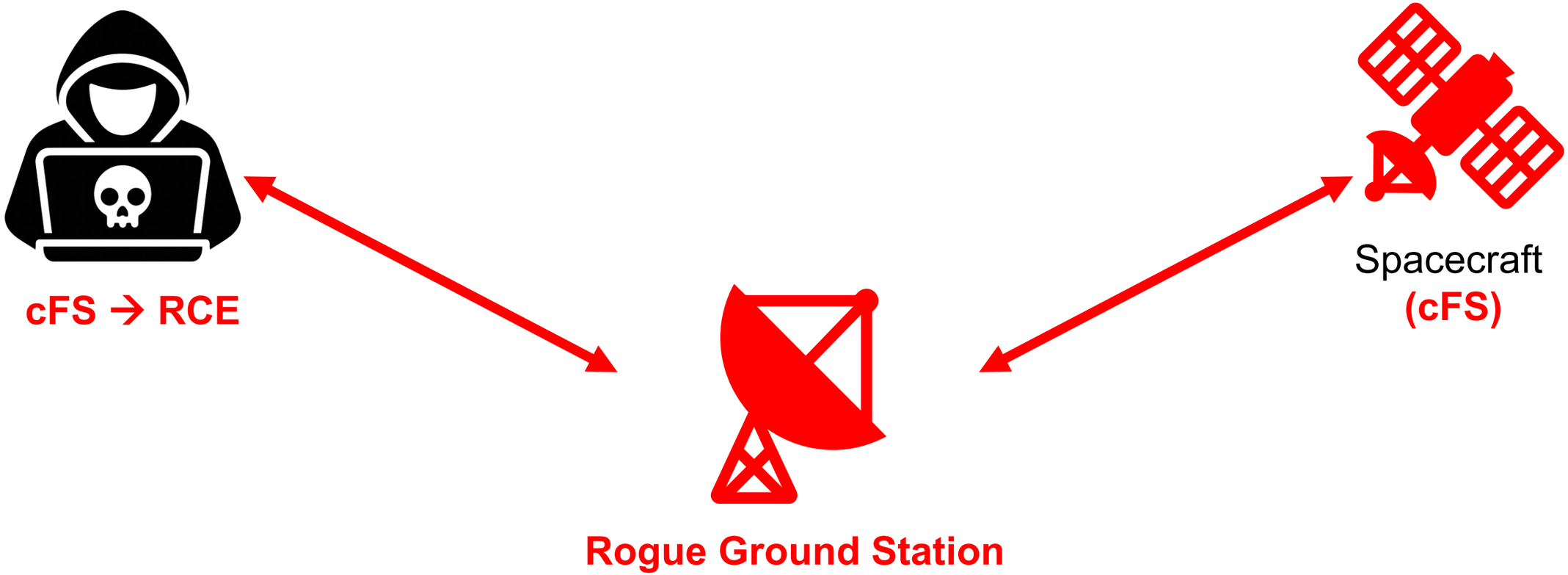
DEMO

NASA cFS DEMO



29 *Write-up: https://visionspace.com/nasa-cfs-version-aquila-software-vulnerability-assessment/*

NASA cFS DEMO



Write-up: https://visionspace.com/nasa-cfs-version-aquila-software-vulnerability-assessment/

Public Disclosures - MCS

Product	CVE
OpenC3 Cosmos v6.0.0	CVE-2025-28380 CVE-2025-28381, CVE-2025-28382 CVE-2025-28384, CVE-2025-28386, CVE-2025-28388, CVE-2025-28389
SAS Yamcs 5.8.6	CVE-2023-45279, CVE-2023-45280, CVE-2023-45281, CVE-2023-46470, CVE-2023-46471, CVE-2023-47311 CVE-2023-45277 CVE-2023-45278
NASA Open MCT 3.1.0	CVE-2023-45884, CVE-2023-45885 CVE-2023-45282

Public Disclosures - MCS

Product	CVE	Severity
OpenC3 Cosmos v6.0.0	CVE-2025-28380	MEDIUM
	CVE-2025-28381, CVE-2025-28382	HIGH
	CVE-2025-28384, CVE-2025-28386, CVE-2025-28388, CVE-2025-28389	CRITICAL
SAS Yamcs 5.8.6	CVE-2023-45279, CVE-2023-45280, CVE-2023-45281, CVE-2023-46470, CVE-2023-46471, CVE-2023-47311	MEDIUM
	CVE-2023-45277	HIGH
	CVE-2023-45278	CRITICAL
NASA Open MCT 3.1.0	CVE-2023-45884, CVE-2023-45885	MEDIUM
	CVE-2023-45282	HIGH

Public Disclosures - Onboard

Product	CVE
NASA cFS Aquila	CVE-2025-25371, CVE-2025-25372, CVE-2025-25374 CVE-2025-25373
NASA Cryptolib 1.3.0	CVE-2024-44910, CVE-2024-44911, CVE-2024-44912
NASA fprime v3.4.3	CVE-2024-55029 CVE-2024-55028, CVE-2024-55030
NASA AIT-Core 2.5.2	CVE-2024-35057, CVE-2024-35058, CVE-2024-35059, CVE-2024-35060, CVE-2024-35061 CVE-2024-35056

Public Disclosures - Onboard

Product	CVE	Severity
NASA cFS	CVE-2025-25371, CVE-2025-25372, CVE-2025-25374	HIGH
Aquila	CVE-2025-25373	CRITICAL
NASA Cryptolib 1.3.0	CVE-2024-44910, CVE-2024-44911, CVE-2024-44912	HIGH
NASA fprime v3.4.3	CVE-2024-55029	MEDIUM
	CVE-2024-55028, CVE-2024-55030	CRITICAL
NASA AIT-Core 2.5.2	CVE-2024-35057, CVE-2024-35058, CVE-2024-35059, CVE-2024-35060, CVE-2024-35061	HIGH
	CVE-2024-35056	CRITICAL

You: Publish CVEs

You: Publish CVEs
Other Researchers:

Exploring Vulnerabilities in the SDLS Implementation of NASA's CryptoLib

Published Dec 18, 2024

Name	CVE	Severity
Keystream Oracle	CVE-2025-46672	LOW
SDLS Bypass	CVE-2025-46673	MEDIUM
Corruption of Key Database	CVE-2025-46674	LOW
Spacecraft Hijacking	CVE-2025-46675	LOW

CryptoLib GitHub Security Advisories

Published Apr 1, Mar 17, Mar 25, 2025

Name	CVE	Severity
Heap Buffer Overflow	CVE-2025-29909	HIGH
Memory Leak	CVE-2025-29910	MEDIUM
Heap Buffer Overflow	CVE-2025-29911	HIGH
Heap Buffer Overflow	CVE-2025-29912	HIGH
Buffer Overflow	CVE-2025-29913	HIGH
Heap Overflow	CVE-2025-30216	CRITICAL
Heap Buffer Overflow	CVE-2025-30356	CRITICAL

Final Thoughts on security in the space sector

- We found this in open source, what about closed source?
- Create rewards for researchers!
- Define security-safety-mission tradeoffs!
- Define mitigation strategies for existing missions!
- What do you do with an insecure mission?
- Space is hard, but space security is not.

Water is wet

Even in space

Thanks!

Andrzej Olchawa

Milenko Starcik

Ricardo Fradique

Ayman Boulaich

VISION SPACE

Black Hat Sound Bytes

- Space is hard, but space security is not.
- Vulnerabilities exist in space systems, like everywhere else.
- Our work covered just open-source; what about closed-source?

References

https://visionspace.com/prototype-pollution-in-nasas-open-mct-cve-2023-45282/

https://visionspace.com/xss-in-nasas-open-mct-v3-1-0/

https://visionspace.com/yamcs-v5-8-6-vulnerability-assessment/

https://visionspace.com/more-xss-and-clickjacking-in-yamcs-v5-8-6/

https://visionspace.com/remote-code-execution-via-man-in-the-middle-and-more-in-nasas-ait-core-v2-5-2/

https://visionspace.com/openc3-cosmos-a-security-assessment-of-an-open-source-mission-framework/

https://visionspace.com/remote-code-execution-and-critical-vulnerabilities-in-nasa-fprime-v3-4-3/

https://visionspace.com/crashing-cryptolib/

https://visionspace.com/nasa-cfs-version-aquila-software-vulnerability-assessment/

https://securitybynature.fr/post/hacking-cryptolib/

https://github.com/nasa/CryptoLib/security