Burning, Trashing, Spacecraft Crashing

A Collection of Vulnerabilities that will End your Space Mission

Andrzej Olchawa, Milenko Starcik, Ricardo Fradique, Ayman Boulaich

DC33 – Aerospace Village

08/08/2025

VISIONSPACE TEAM

Milenko Starcik

Head of Cybersecurity

Andrzej Olchawa

Cybersecurity Engineer

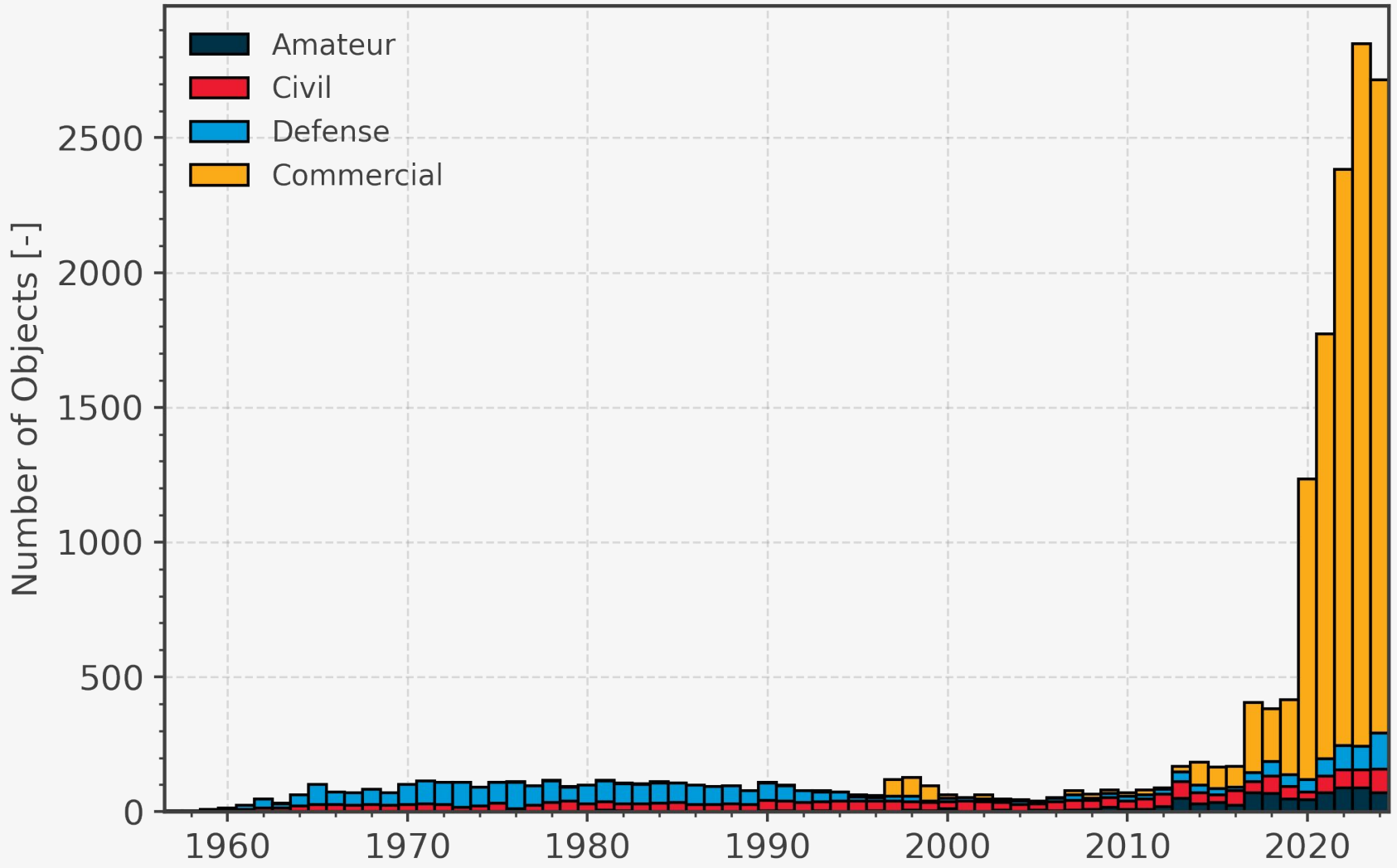
Ricardo Fradique

Cybersecurity Engineer

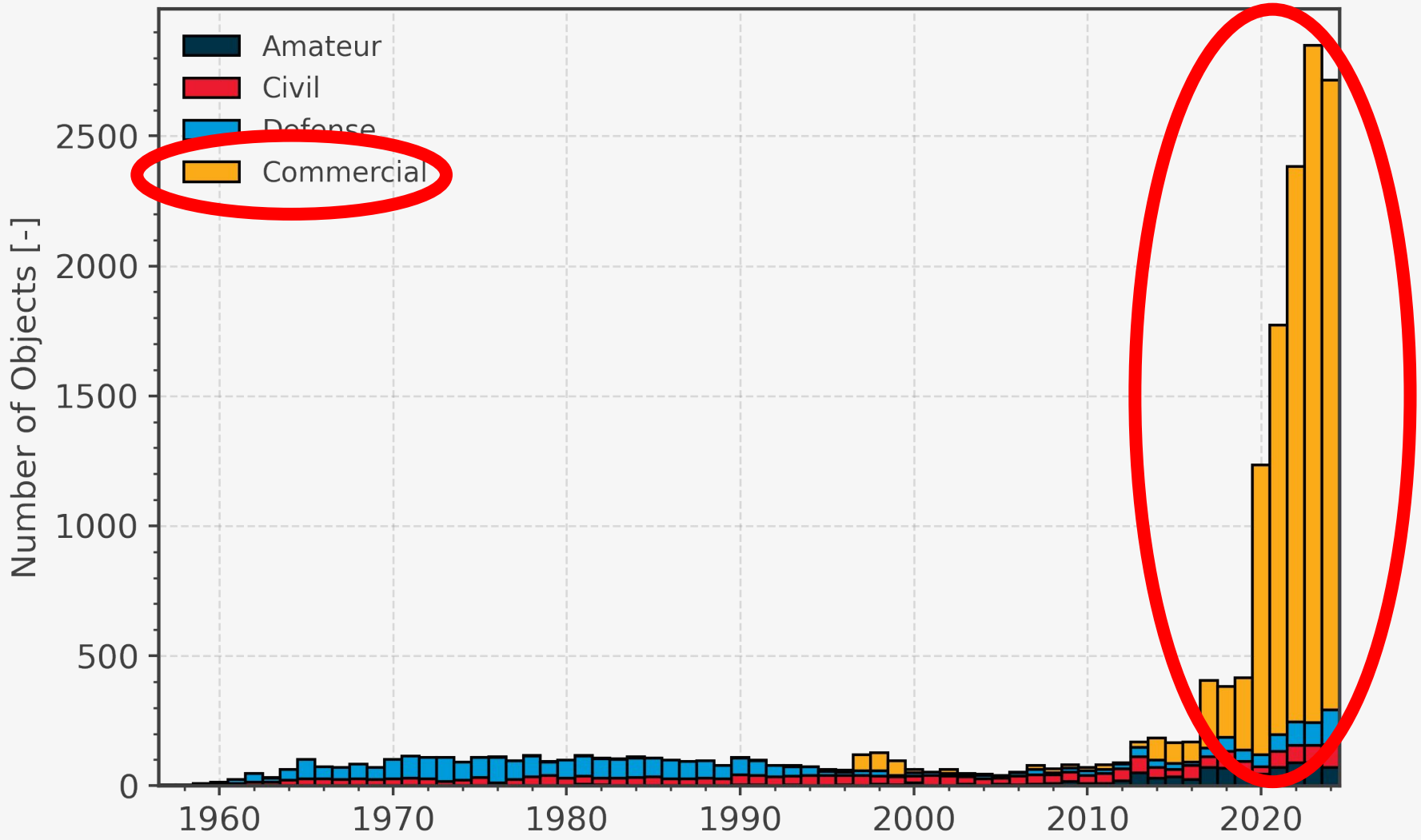
Ayman Boulaich

Cybersecurity Intern

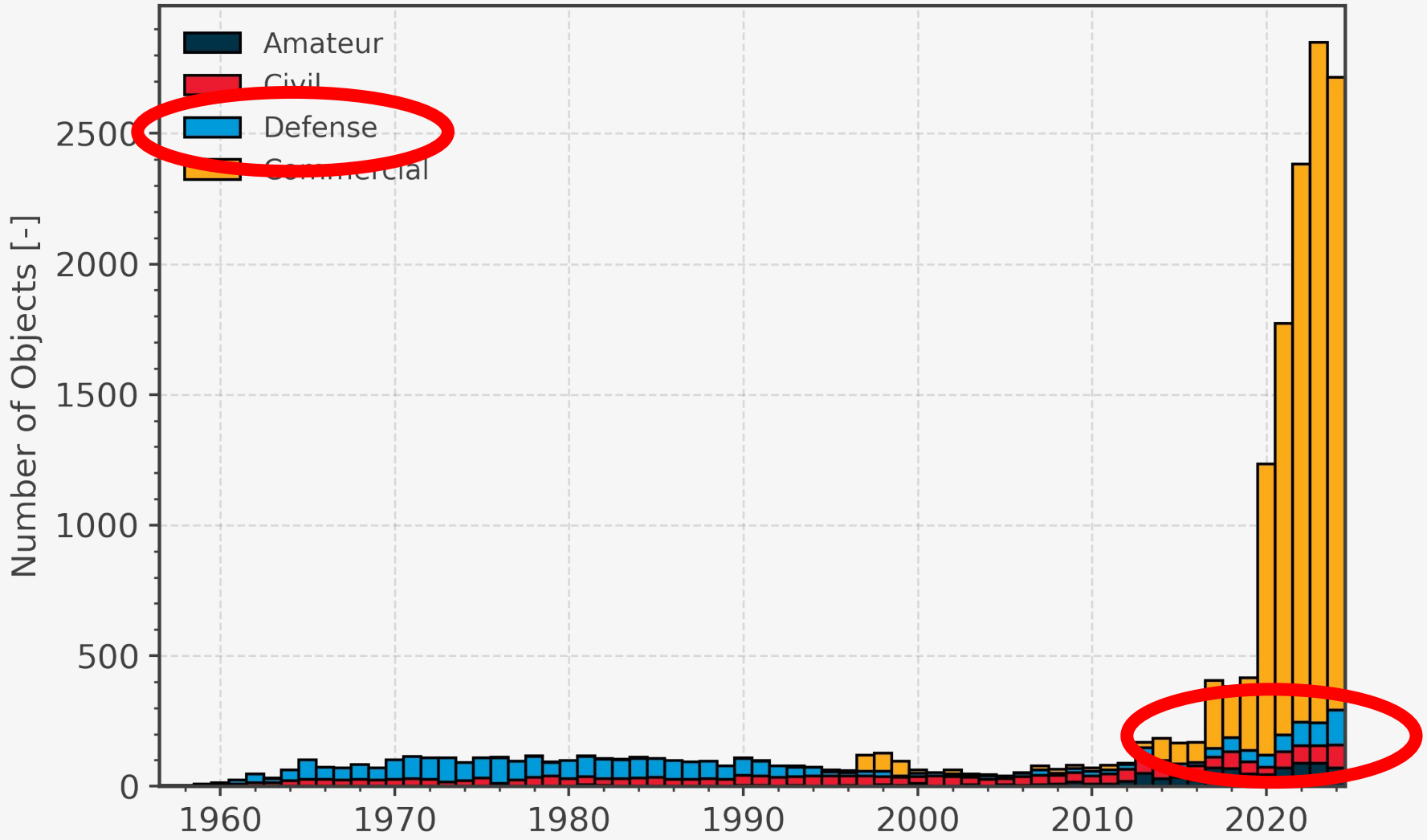
Satellites launched to LEO per year

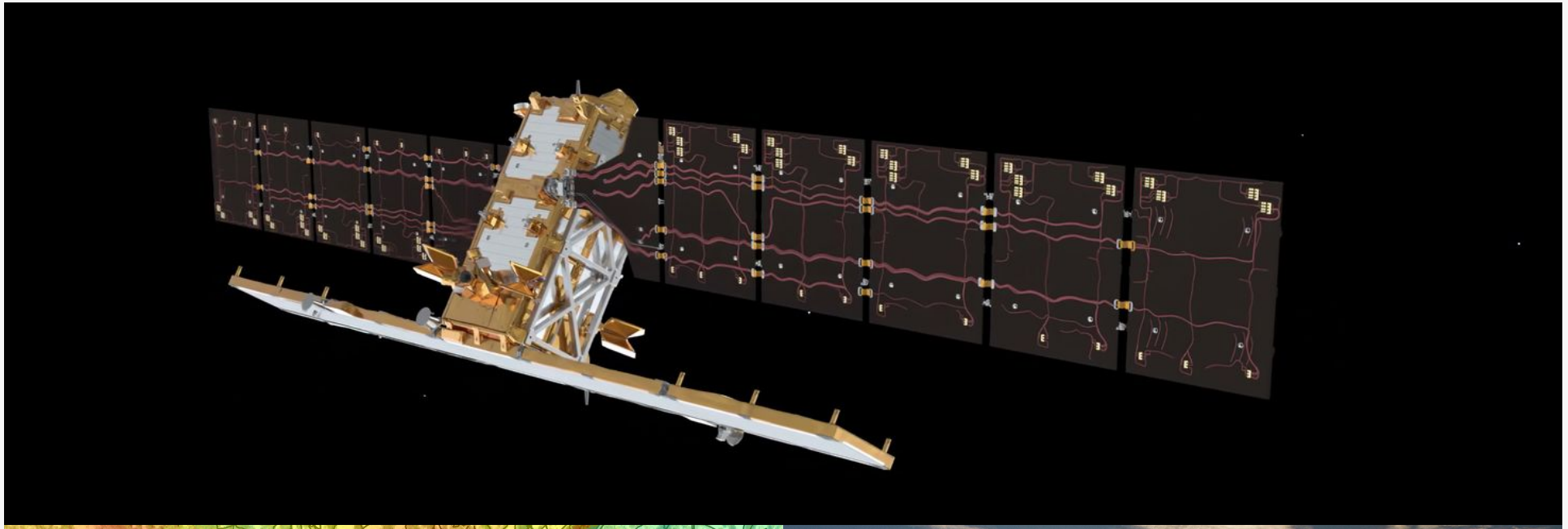


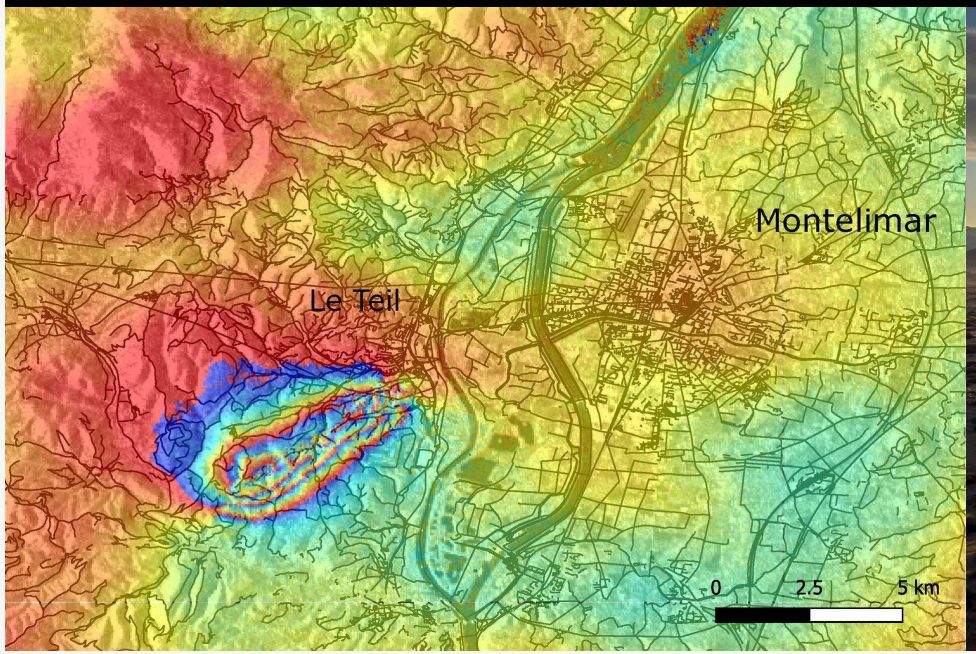
Commercialization



Re-Militarization






Montelimar
Le Teil
0
2.5
5 km

Disabling a Satellite

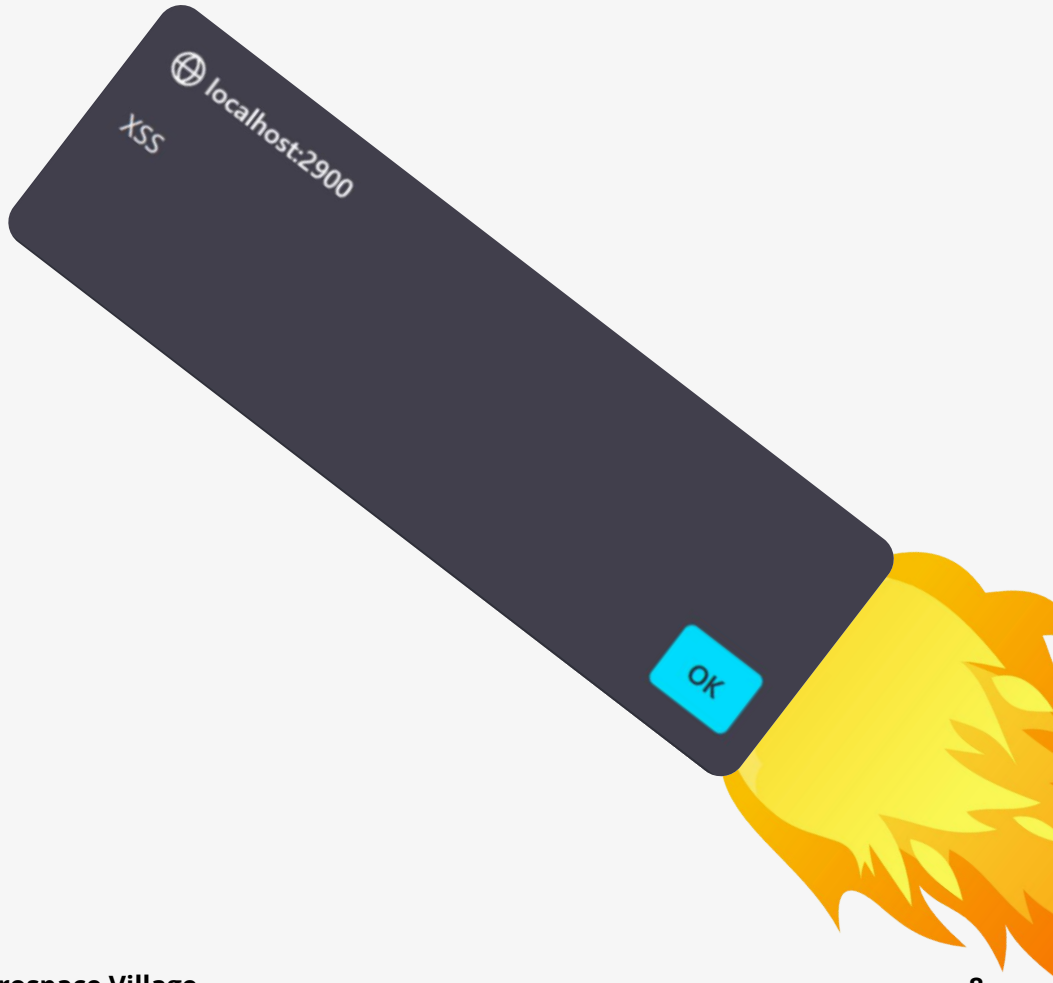
What you expect

What we found

Disabling a Satellite

What you expect

What we found



Product	CVE	Severity
NASA cFS Aquila	CVE-2025-25371, CVE-2025-25372, CVE-2025-25374	HIGH
	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
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
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
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

Product	CVE	Severity
NASA cFS Aquila	CVE-2025-25371, CVE-2025-25372, CVE-2025-25374	HIGH
	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
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
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
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

OpenC3 COSMOS Demo

SAS YAMCS DEMO

NASA cFS Demo

You: Publish CVEs

You: Publish CVEs
Other Researchers:

Exploring Vulnerabilities in the SDLS Implementation of NASA's CryptoLib

Published Dec 18, 2024

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

CryptoLib GitHub Security Advisories

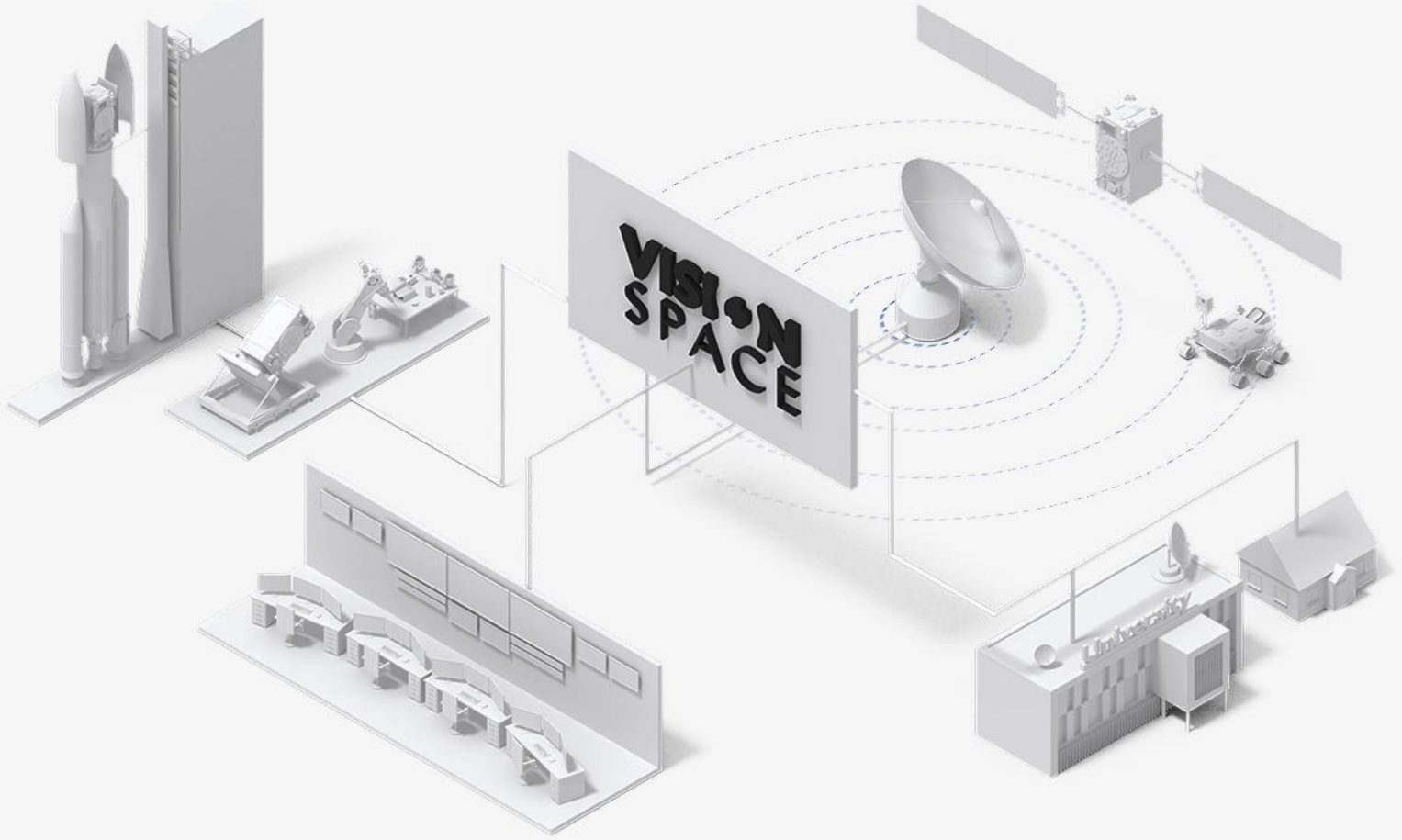
Published Apr 1, Mar 17, Mar 25, 2025

Name	CVE ID
Heap Buffer Overflow	CVE-2025-29909
Memory Leak	CVE-2025-29910
Heap Buffer Overflow	CVE-2025-29911
Heap Buffer Overflow	CVE-2025-29912
Buffer Overflow	CVE-2025-29913
Heap Overflow	CVE-2025-30216
Heap Buffer Overflow	CVE-2025-30356

Final Thoughts

- Security training and awareness
- Space mission lifecycle security engineering
- Security-safety-mission tradeoffs
- Mitigation strategies for existing missions
- Software security maintenance

Contact



Milenko Starcik
Head of Cybersecurity
milenko.starcik@visionspace.com

Andrzej Olchawa
Cybersecurity Engineer
andrzej.olchawa@visionspace.com

VisionSpace Technologies GmbH

Robert-Bosch-Strasse 7
64293 Darmstadt
Germany

visionspace.com