SnT

Interdisciplinary Centre for
Security, Reliability and Trust

CritiX Space Safety and Security Lab: a path towards trustworthy space systems

Rafał Graczyk

uni.lu
UNIVERSITY OF
LUXEMBOURG

Agenda

1. **group intro**
2. **space systems security intro**
   - different types of attacks at various parts of the system
3. **need for research infrastructure**
   - to experiment
   - to educate
4. **the CritiX S^4 Lab**
   - goals and capabilities
   - functions
   - intended use

SnT

CritiX

UNIVERSITY OF LUXEMBOURG

CritiX Mission

FOUR OBJECTIVES

to enable resilient computing in a wide range of application areas:

01
ULTRA-RESILIENT
Minimal Roots-of-trust and Enclaves

02
HYBRIDISATION-AWARE
Distributed, Algorithms, Models, and Architectures

03
HIGH-CONFIDENCE
Vertical Verification of Mid-sized Software

04
PRIVACY-AND INTEGRITY-PERSERVING
Decentralised Data Processing

RESILIENT COMPUTING

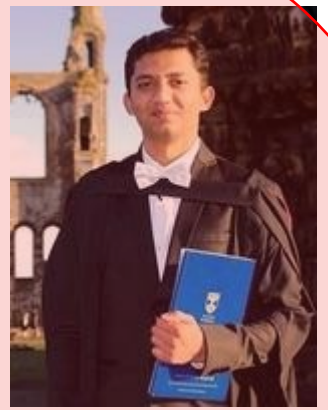
- Autonomous Vehicles and Resilient, Adaptive Control
- Internet/Cloud
- eHealth
- Fintech
- Resilient Space Systems

CritiX – the Critical and Extreme Security and Dependability Research Group

Associate Prof. Marcus Völp
Microkernels, Real-Time Systems

Dr. Rafal Graczyk
Space Systems

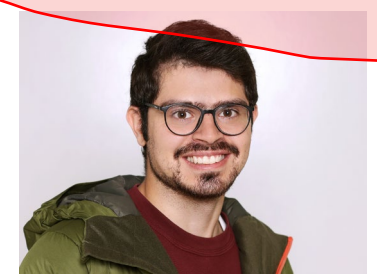
Gelmar



Saad Memon
Radiation Tolerance

Dr. Federico Lucchetti
AI, Autonomous Driving

Dr. Ozgur Ceyhan
Math, Crypto



Amin Naghavi
Real-Time Systems

Aleksandar Matovic
Resilient Control

Dr. Julio de Mendoca
SDN, Petri Nets

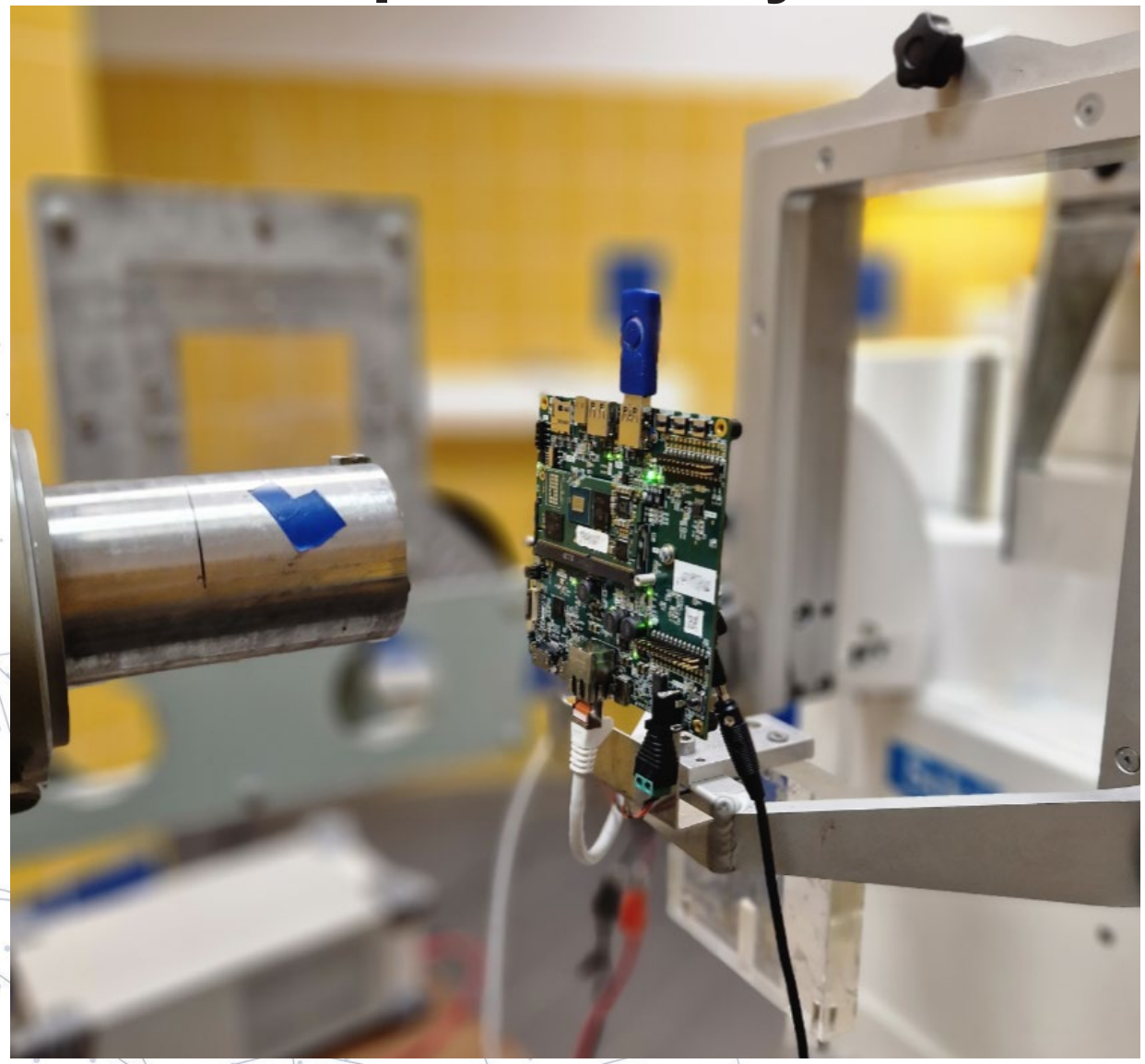
Dr. Mouhammad Sakr
Formal Methods,
Bounded Model Checking

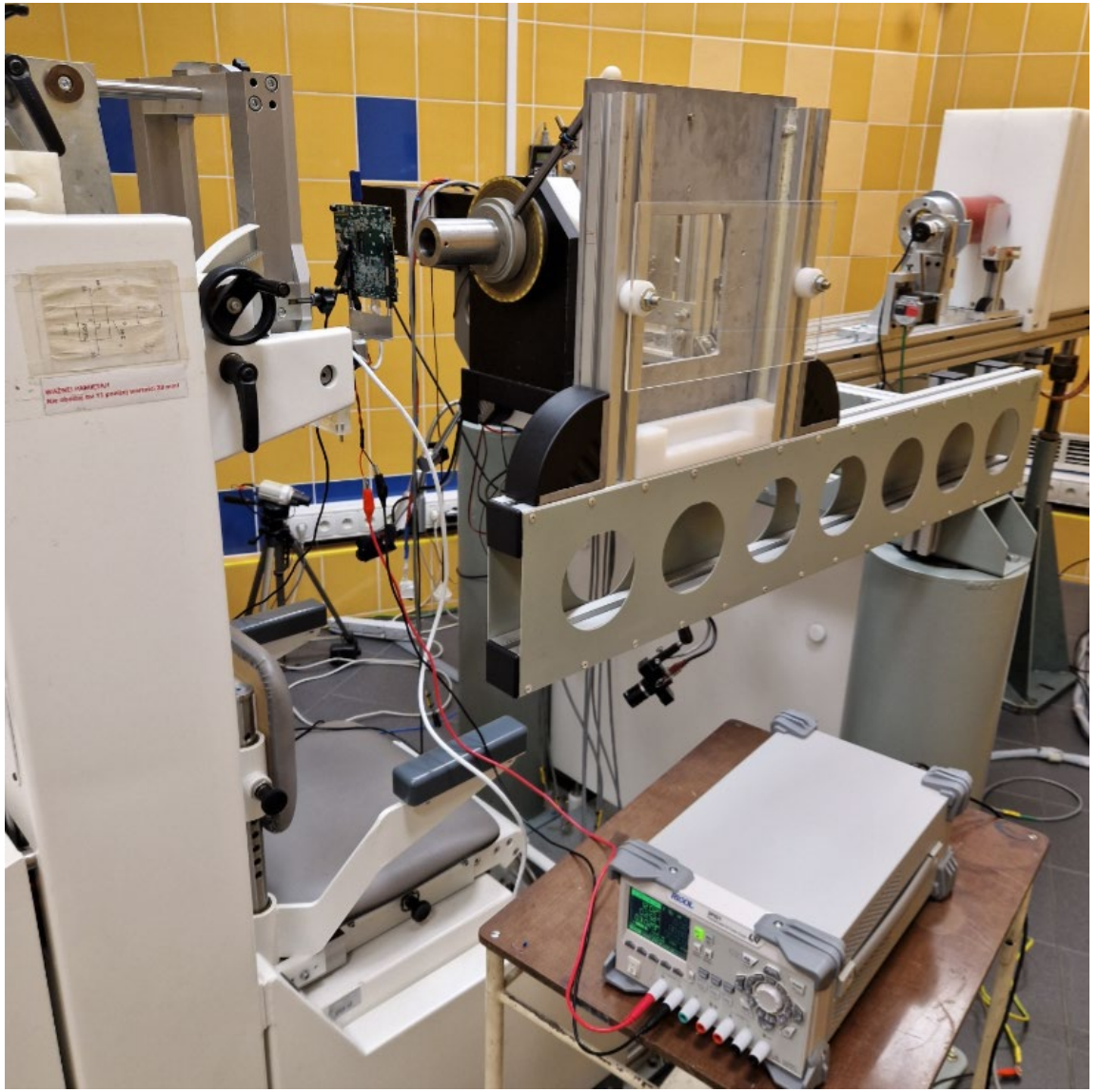
Douglas Simoes Silva
Threat Adaptive Systems

Wassim Yahyaoui
Clustered Consensus

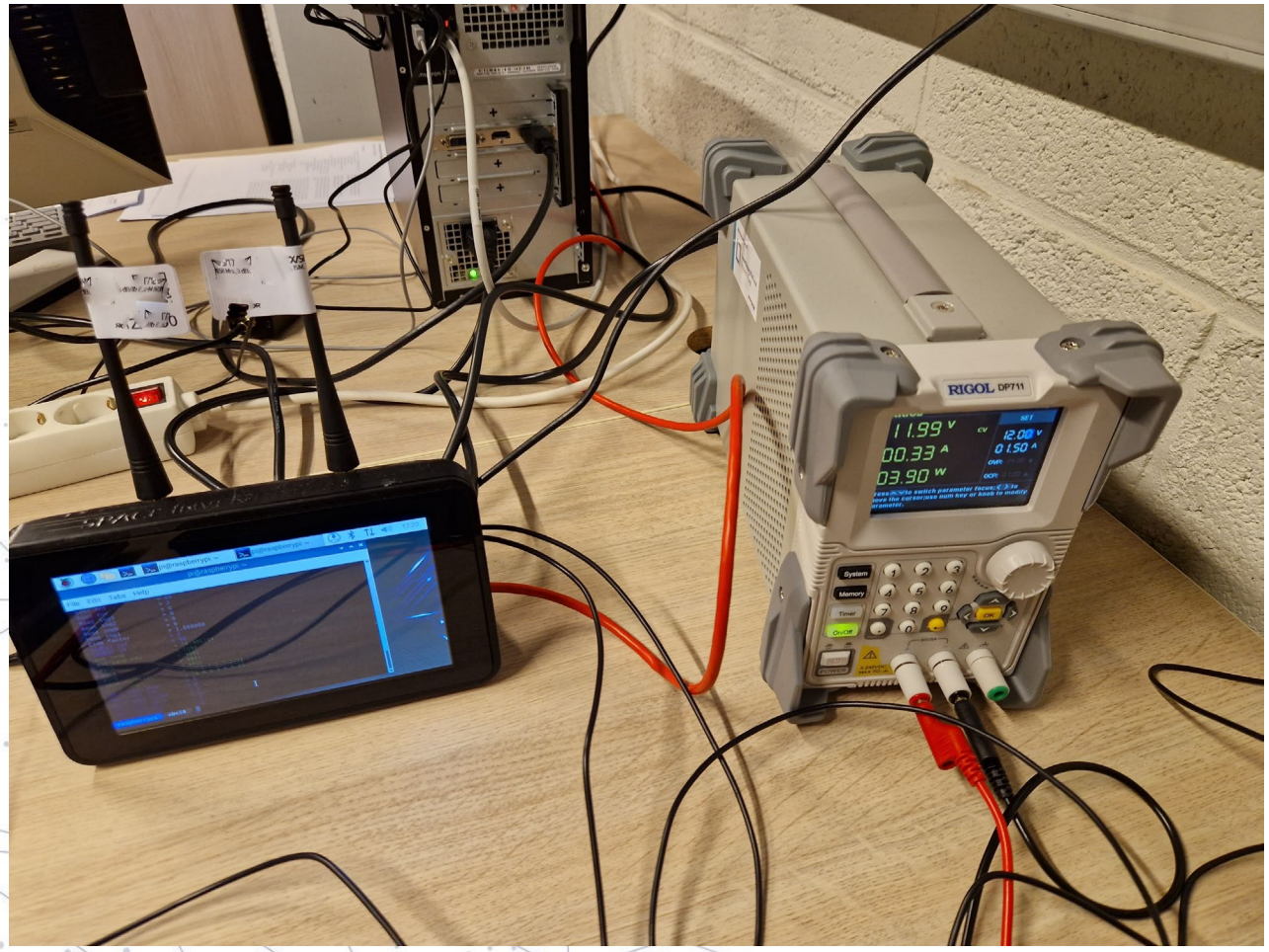
uni.lu | SnT

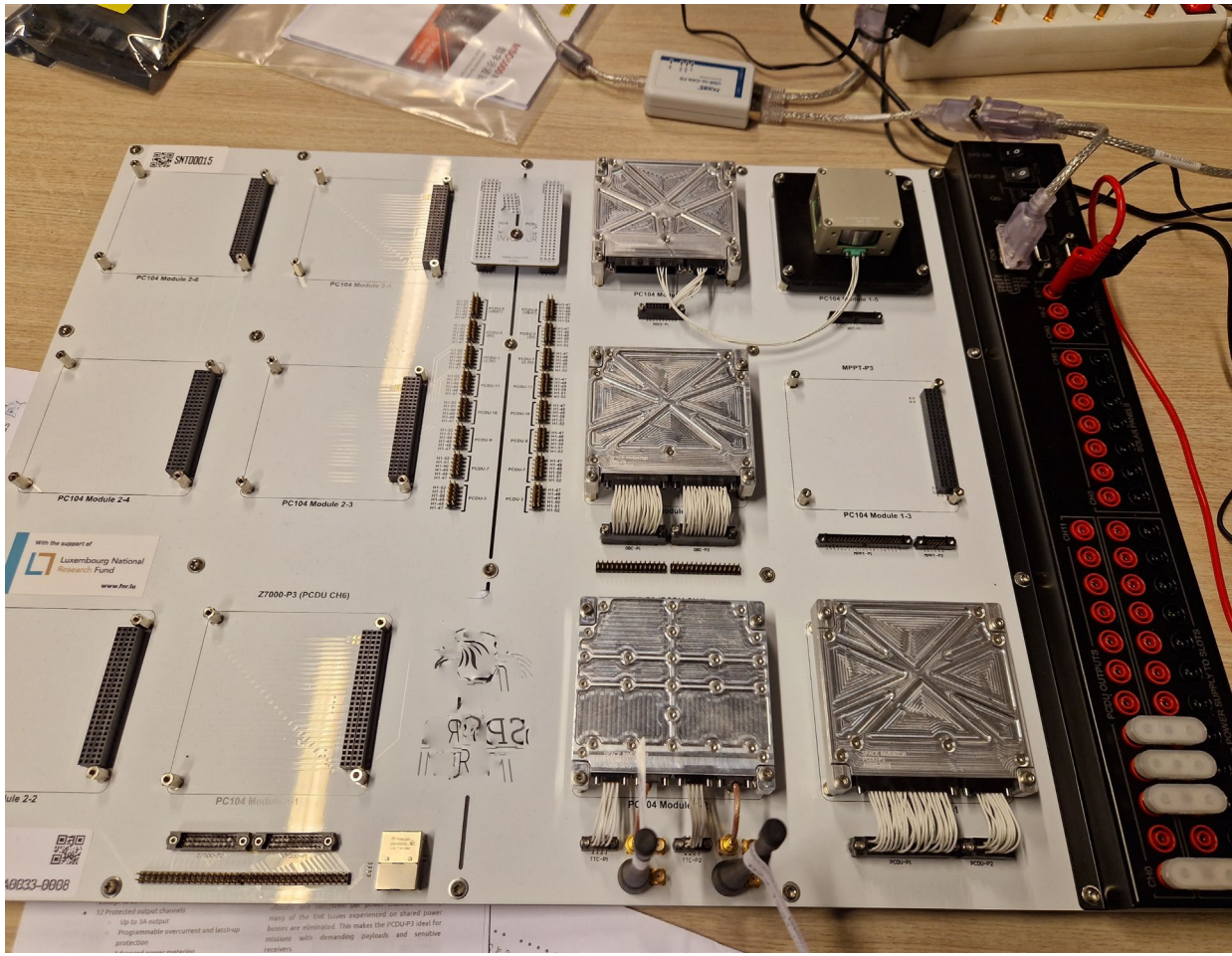
CritiX Space Safety





CritiX Space Security






SNT
Into the Space
Systems (in)Security
UNIVERSITY OF
LUXEMBOURG

The “High Ground” fallacy

In military doctrines **Space Assets** are considered a **High Ground**...

... this has also spilled over to civilian sector.

Let’s compare old and modern High Grounds

Castle	Satellite
• hard to reach and hit	• quite easy to reach and hit
• easy to defend	• challenging to defend
• effective to fight back	• no way to fight back
• oversees the surroundings	• oversees what is below, .. for a while
• controls the area	• ?
• built using local resources	• have to take all resources on a mission
• resupplied using local resources	• very rarely resupplied (for now)

J. Oberg, Space Power Theory, UASF Academy, 1999

Sanctuary lost? Yes, if we go digital.

classic threats

- easy to attribute
- sophisticated technology
- expensive
- efficient in non-networked env.

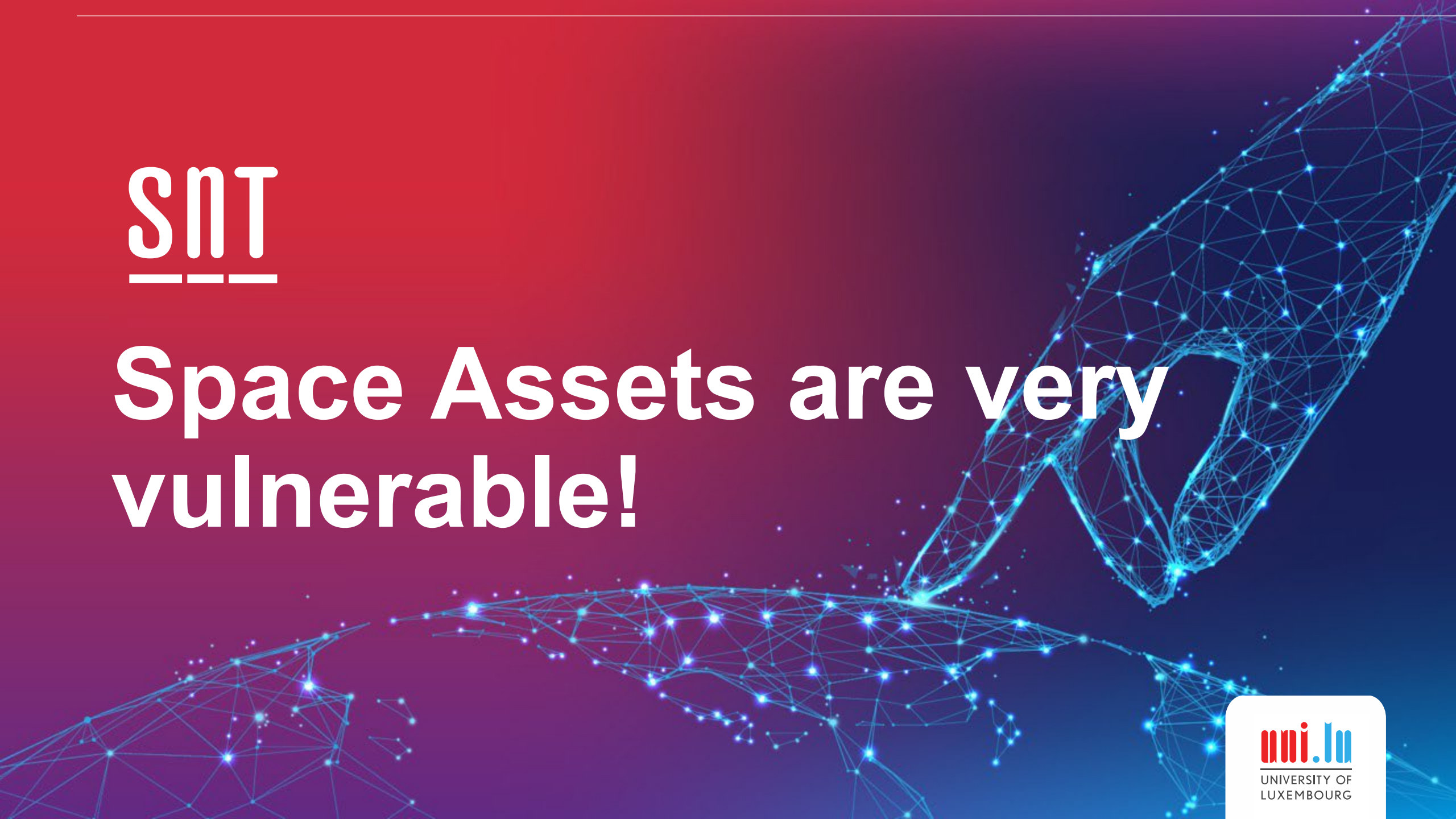
high entry barrier

cyber threats

- hard to attribute
- common technology
- inexpensive
- efficient in networked environment

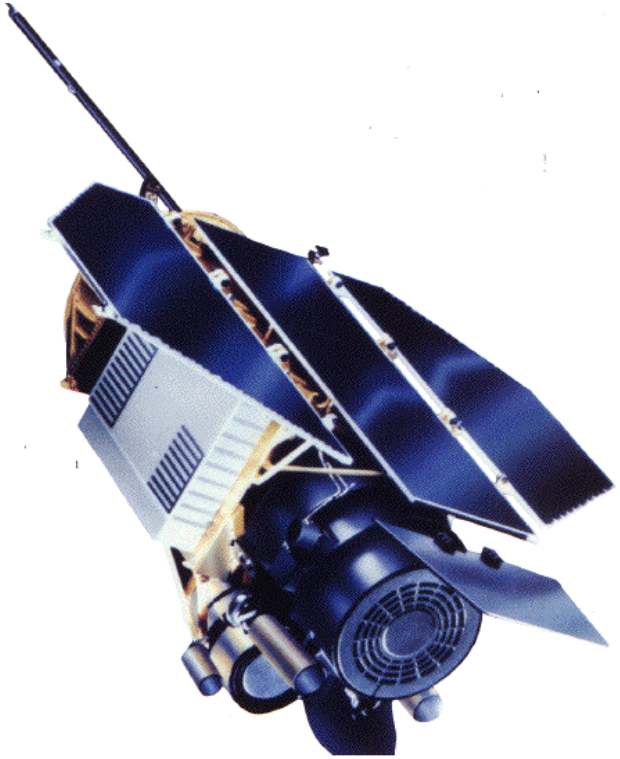
low entry barrier

...best thing about cyber is that results may also be physical and large scale!


SNT
Space Assets are very vulnerable!
UNIVERSITY OF LUXEMBOURG

Curious death of ROSAT (1998)

2008: NASA investigators were reported to have found that the ROSAT failure was linked to a cyber-intrusion at Goddard Space Flight Center.

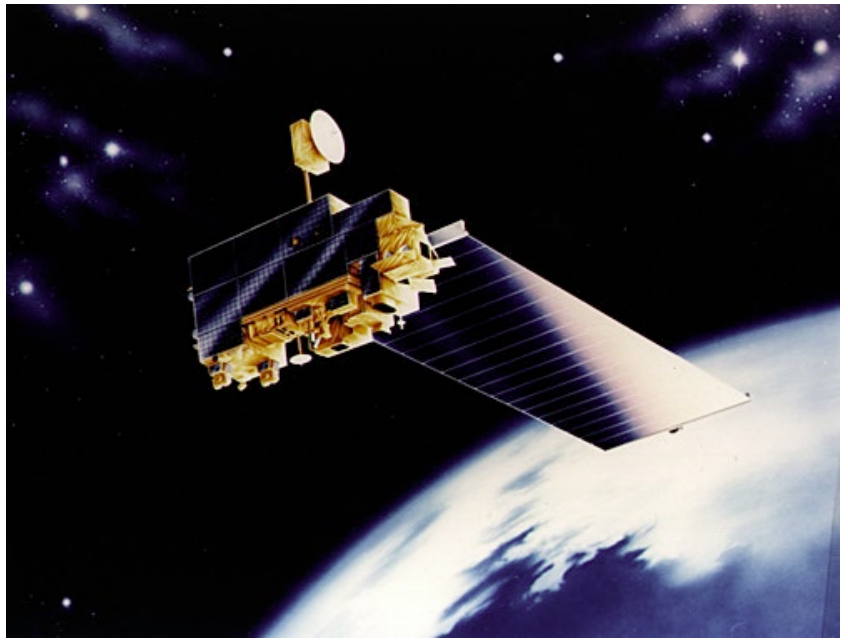


1999: advisory report by Thomas Talleur, senior investigator for cyber-security at NASA:

- series of attacks from Russia that reached computers in the X-ray Astrophysics Section
- took control of computers used for the control of satellites, not just a passive "snooping" attack

Reference: Network Security Breaches Plague NASA, Newsweek / Bloomberg / BusinessWeek, 2008
https://www.cs.clemson.edu/course/cpsc420/material/Papers/NASA.pdf
http://www.kepstein.com/2008/11/20/network-security-breaches-plague-nasa/

Landsat, Terra EOS (2008 - 2009)



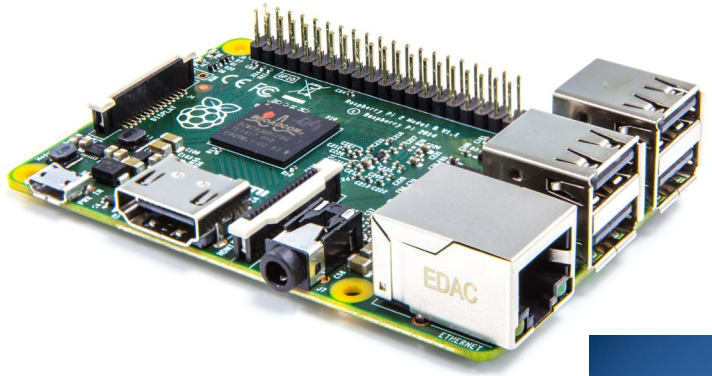
06 & 10.2008: the spacecraft was targeted by hackers who gained unauthorized access to its C&C systems, but (as is claimed by US officials) did not issue any commands.

- last from series of similar attacks that were launched on Landsat and Terra EOS satellites.
- No details whether it was rogue GS or hack into existing one (polar regions)

Reference: 2011 Report to Congress of the U.S.-China Economic and Security Review Comission, November 2011 https://www.uscc.gov/annual-report/2011-annual-report-congress/

NASA JPL breach (2011 & 2018)

- compromised accounts of high privilege
- hackers had full system access for months
- explore NASA networks beyond JPL

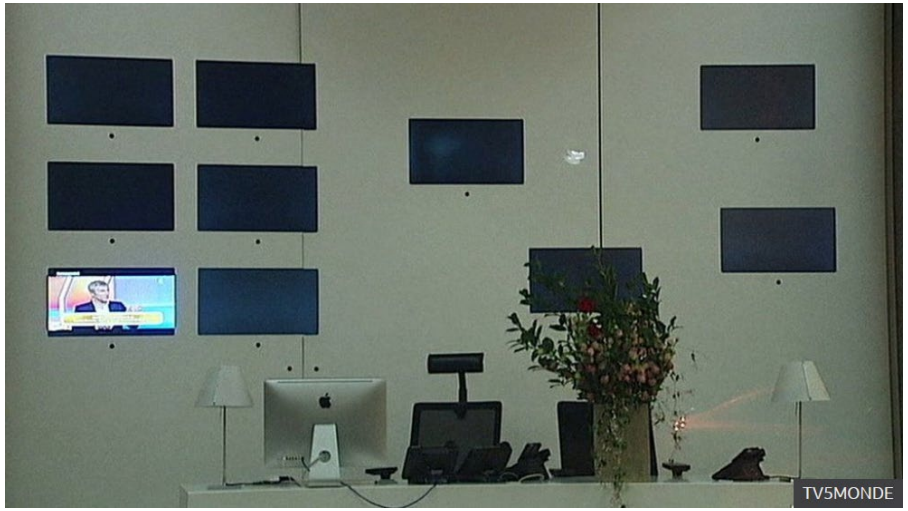


- the same happened in 2018
- unauthorized RPi plugged into facility network -> WiFi access for hackers
- access to confidential documents
- access to DSN
- > 14 months, 500 MB of ITAR-controlled docs stolen

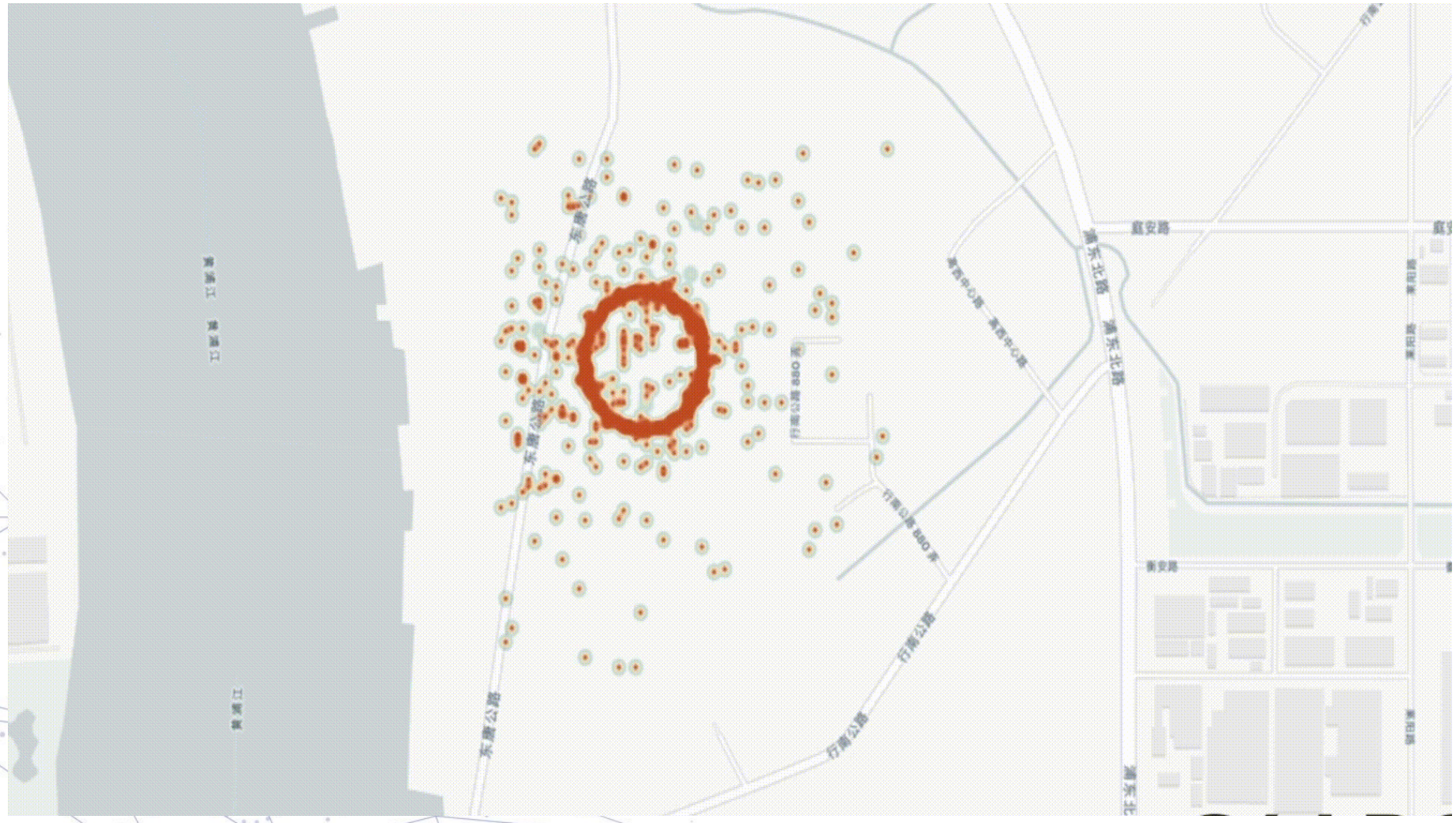
Mayhem at TV5Monde (2015)

- in 2015 TV5Monde experienced devastating attack on its broadcast facilities
- all 12 channels were down, for many hours
- months before attack internal station networks were thoroughly mapped
  - investigated the broadcast process
  - listed the equipment
- grand finale involved deployment of malicious software that targeted critical elements of ground stations **causing permanent hardware damage**

- APT28 *maskirovka* as Cybercaliphate



Basic GPS spoofing (2019)



Positions of ships reported through AIS became clearly erroneous:

- ships moved inland
- sailing in circles

- first spotted in Shanghai on Yangtze

It took a while to realize there might be a problem

2007 Terra

2009 JPL

2010 NASA

2011 JPL

2015 TV5

2018 JPL

2020 SPD-5

2020 DE, FR

TABLE III
SUMMARY OF PUBLICLY KNOWN SPACE INFRASTRUCTURE SECURITY INCIDENTS [5], [6], [7]

Year	Incident	Remarks
1998	ROSAT	Scientific satellite payload permanent failure coincidental with cyber-intrusion to mission control center, incident report classified [76], [77]
1999	Skynet	British military communication satellite allegedly taken over and ransom requested, lack of solid, public, evidence of incident [78], [79]
2000	GPS jamming during military trials	British and US tank had navigation problems during Greek trials. GPS jammers deployed by French security [80]
2003	Ames Research supercomputer shut down to halt intrusion	Swedish national persecuted, estimated costs > 1MUSD [81]
2003	TELSTAR-12 uplink jamming	TELSTAR-12 uplink was jammed, by source located in Cuba, during Operation Iraqi Freedom to prevent Voice of America broadcast over Iran [82]
2005	Sri Lankan rebels hijack satellite communications	Liberation Tigers of Tamil Eelam broadcast pirated TV & radio services to several countries [?]
2006	Data breach and multiple intrusions	NASA forced to block emails, Shuttle operations plans leaked [83], [84]
2007	Landsat-7	First unauthorized attempt to access the space segment [85], [86]
2008	Landsat-7 & Terrasat EOS interference	Very well documented hack attempt, large sophistication of adversary [85], [86]
2008	Worm infecting laptops on ISS	Brought by a Russian astronaut on Windows XP laptop. Malware quickly spread among other computers (although mission-critical equipment was safe) [87], [88]
2009	JPL data breach and malware spreading in NASA mission networks	Theft of 22GB of export-restricted data; thousands of connection set to external networks [89]
2009	BBC broadcast in Farsi disrupted	Telecommunication satellite jammed [90]
2009	NASA Goddard Center information leaked	Paid Earth imagery datasets posted online for free [81]
2010	GPS jamming by N. Korea	Multiple locations affected in S. Korea including Incheon International Airport. Aircraft had to rely on alternative navigation instruments. Incidents repeated couple of times in following years [91]
2010	NASA intrusions	Data destroyed or access restricted, 0.5 MUSD damage to Atmospheric Infrared Sounder (AIRS) program [92]
2011	NASA JPL breach	Hackers gained full access to JPL systems [93], [92]
2011	European communication satellite jamming	Deutsche Welle jammed on DeHotbird 8 satellite [94]
2011	NASA ISS command and control data leak	An un-encrypted NASA laptop was stolen. It contained the command sets, as well as, control algorithms for ISS [95], [92]
2011	JAXA H-2A Transfer Vehicle design leak	Virus infected laptop containing critical data [96]
2012	NASA and ESA identity and authentication data hacked and published	Around one thousand employees personal information leaked and posted in internet [97]
2012	JAXA Epsilon rocket design leak	Virus infected laptop containing critical data [98]
2014	DLR breach and data theft	Targeted malware found across DLR computers. Theft linked to China APT groups [99]
2014	Mulitple channels broadcast disrupted over Ethiopia	Arabsat telecommunication satellite jammed [100]
2014	NOAA satellite weather imagery service disrupted	Data flow from satellites affected by hack attributed to Chinese APT, systems forced offline [101], [102]
2015	*Turla* satellite communication links hijacks	*Turla* hacker group with links to FSB - hijacking internet services of older commercial satellites [103], [104], [105]
2015	*APT28* hacked French TV5Monde television	A professional, coordinated attack that disabled the TV broadcaster for couple of hours. It took months to fully replace destroyed equipment and return to regular operations [106]
2018	JPL intrusion	500 MB of critical documents leaked, unauthorized access to deep space network, operations affected for many months, [107], [108]
2018	malware in ISRO launch segment	suspected, ISRO named it false positive [109], [110], [111]
2018	DoD contractors hacked	Security breach with the possibility to exercise the control over satellite by hackers, data traffic disruptions. Additionally confidential design data on submarines and high fidelity satellite imagery stolen [112], [113]
2019	Advanced GPS signal spoofing in China	Ships GPS positions, reported by maritime satellite AIS system [114], [49]
2019	Successful attack on autonomous car navigation by GPS spoofing	[115]
2020	Worldwide advanced GPS signal spoofing	Ships located physically in waters near Norway, Libya, Malaysia, and Russia reported via AIS to sailing in circles off the San Francisco coast[116], [117]

2001 Rumsfeld's warning

2019 NATO

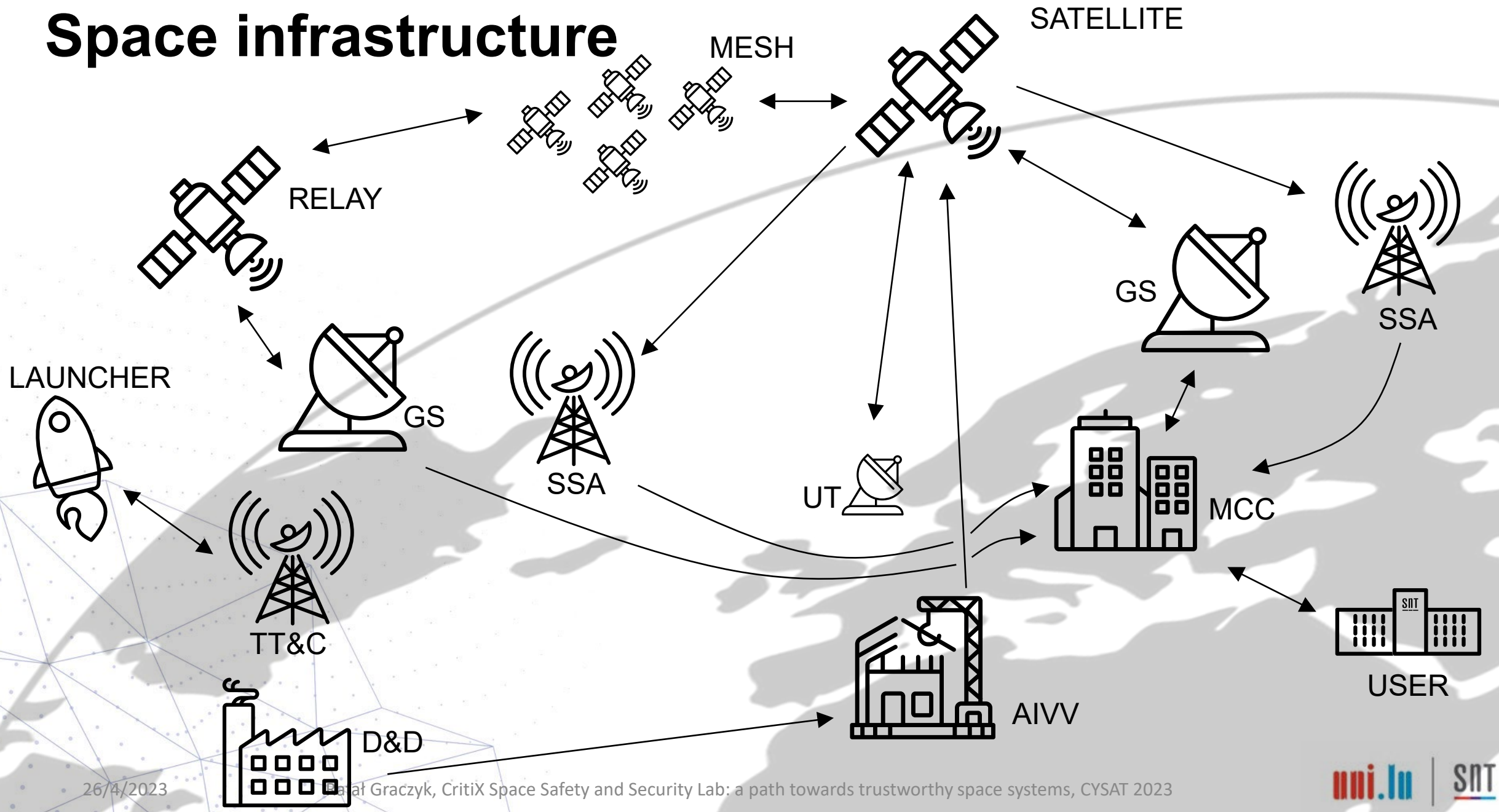
2019 USSF

SNT

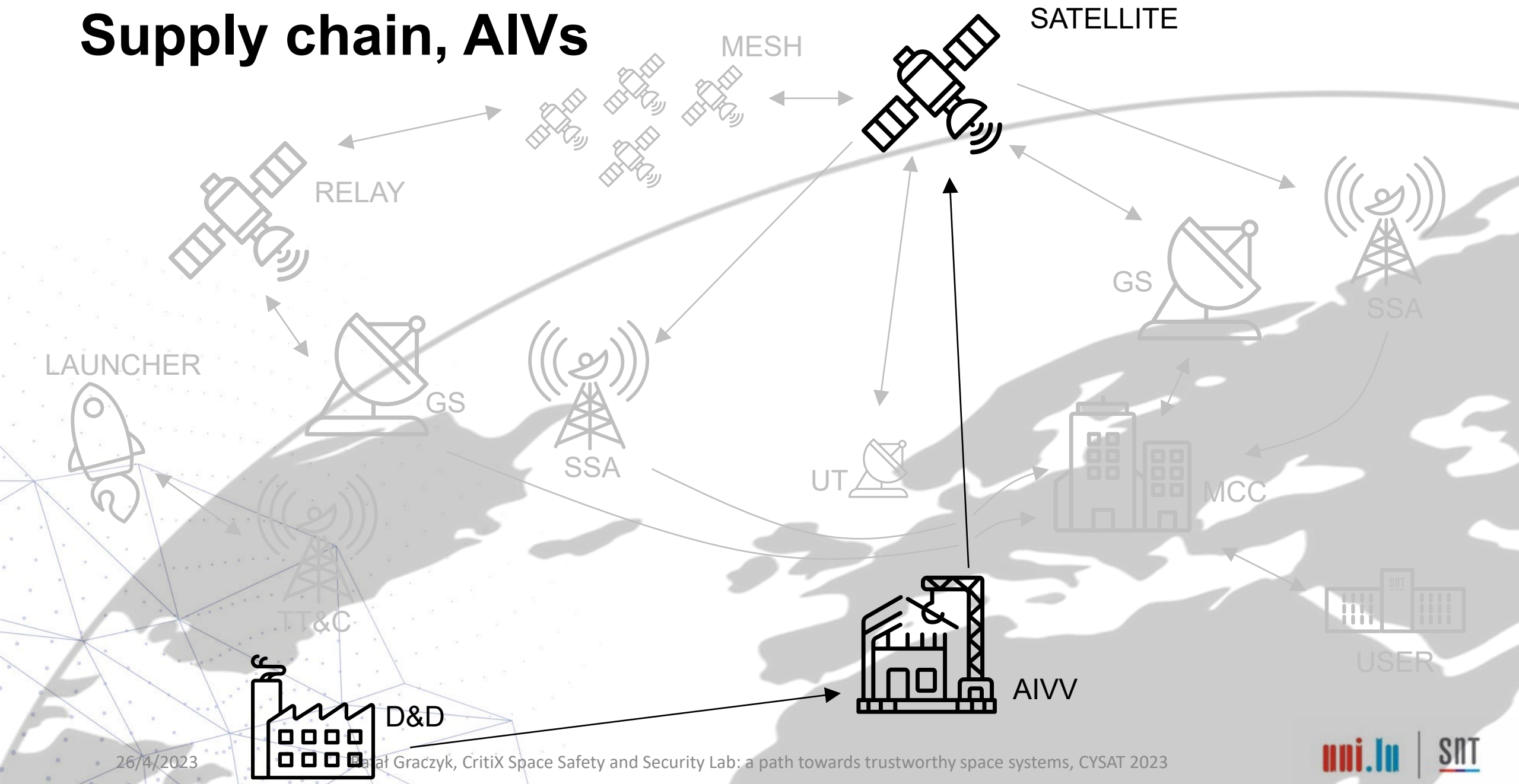
Space Infrastructure Attack Vectors

UNIVERSITY OF LUXEMBOURG

Space infrastructure



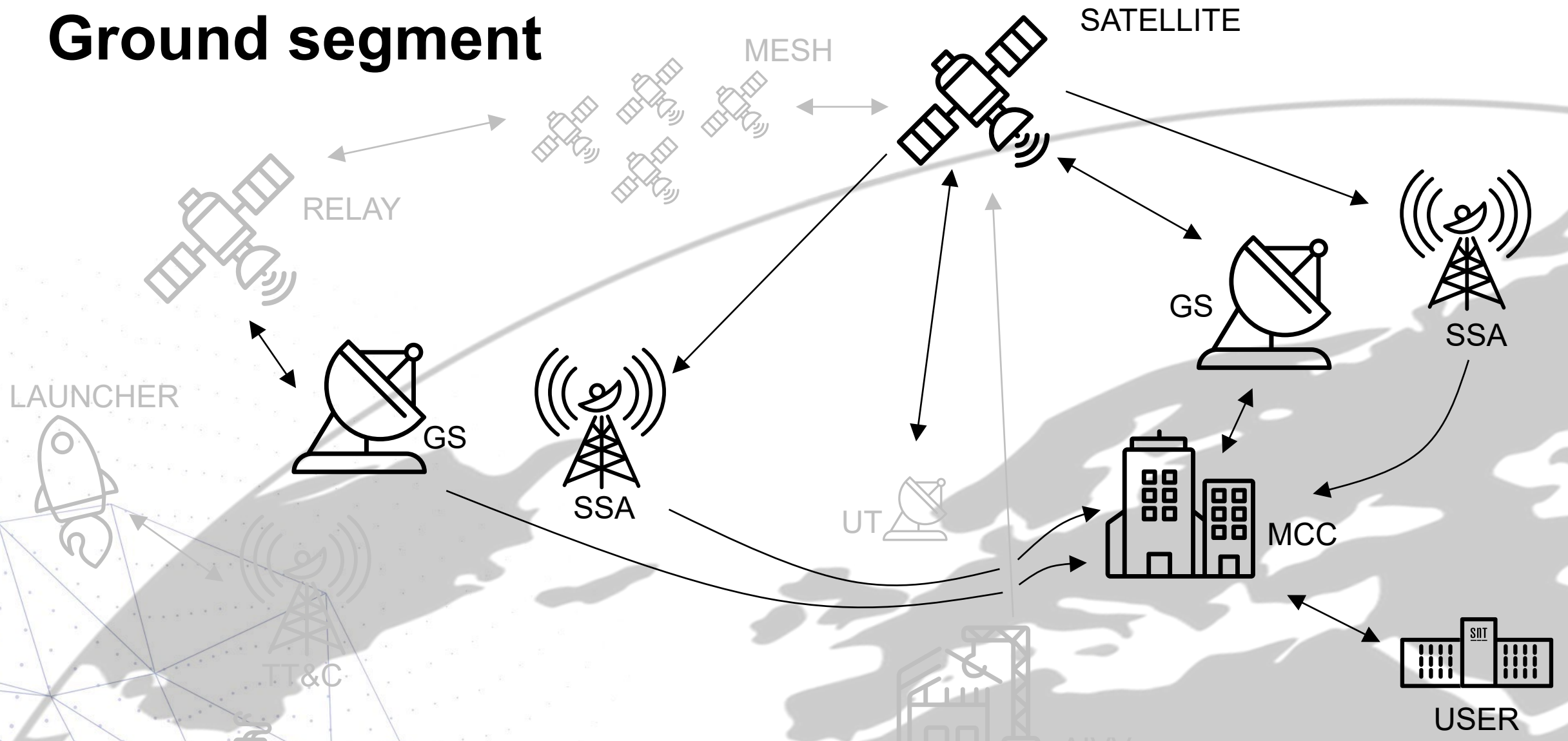
Supply chain, AIVs



Attack Vectors – Supply Chain and AIV's

Loss of \ Affecting	supply chain	assembly & integration	test
confidentiality	design / spec theft	documentation theft	test plan / results theft
integrity	component tainting design modification	documentation modification	test specification modification test equipment setting modification
availability	component supply disrupt design deletion	documentation deletion facility unavailability	test equipment unavailability test results deletion

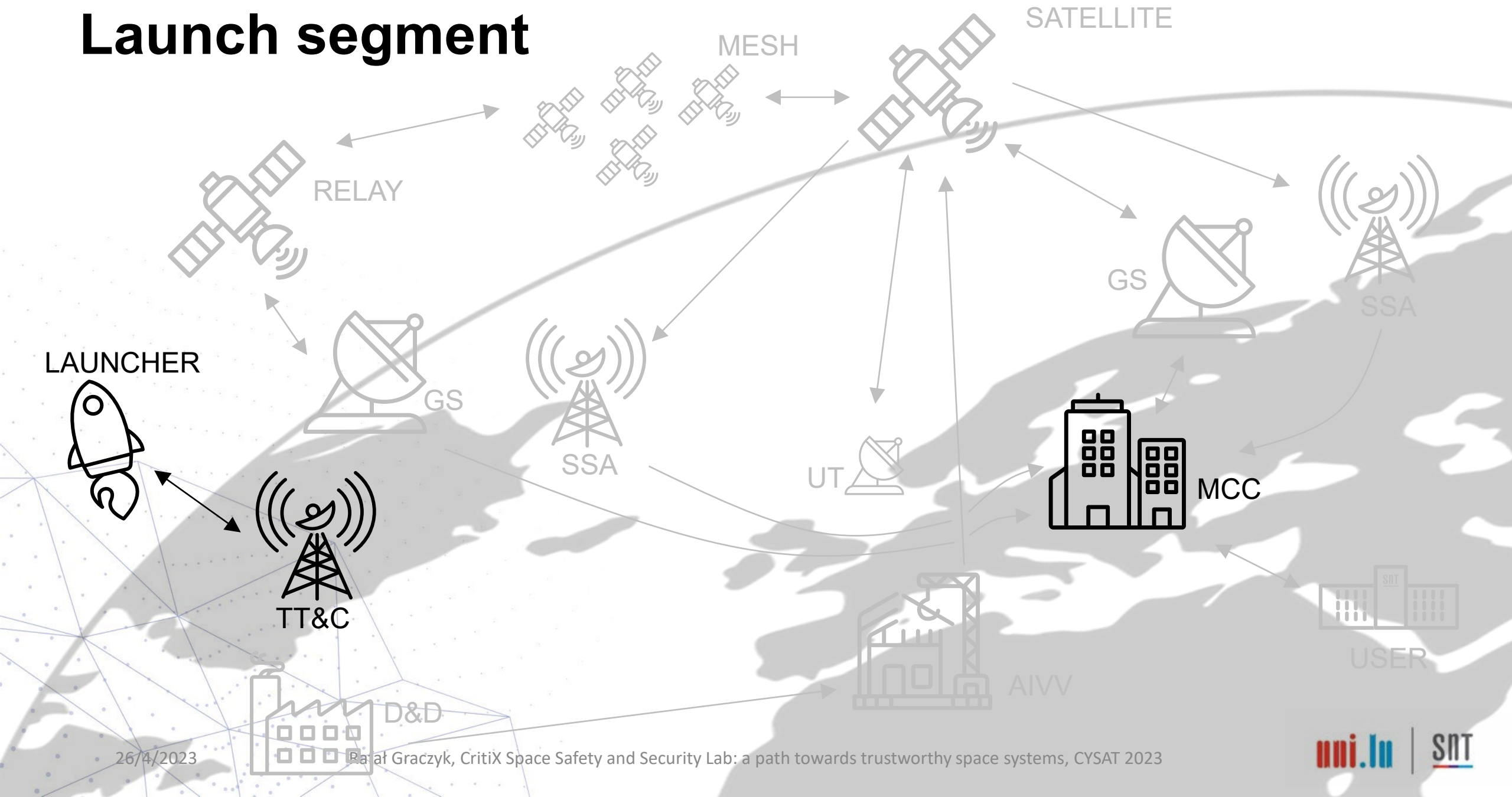
Ground segment



Attack Vectors – Ground segment

Loss of \ Affecting	ground station	mission control	space traffic mgmt
confidentiality	eavesdropping tracking	eavesdropping	tracking
integrity	masquerading message replay	modification of commands modification of telemetry	MITM attack on ephemerides distribution catalogue modification
availability	denial of service jamming	denial of service facility unavailability	tracked object deletion for data pool tracking facility unavailability

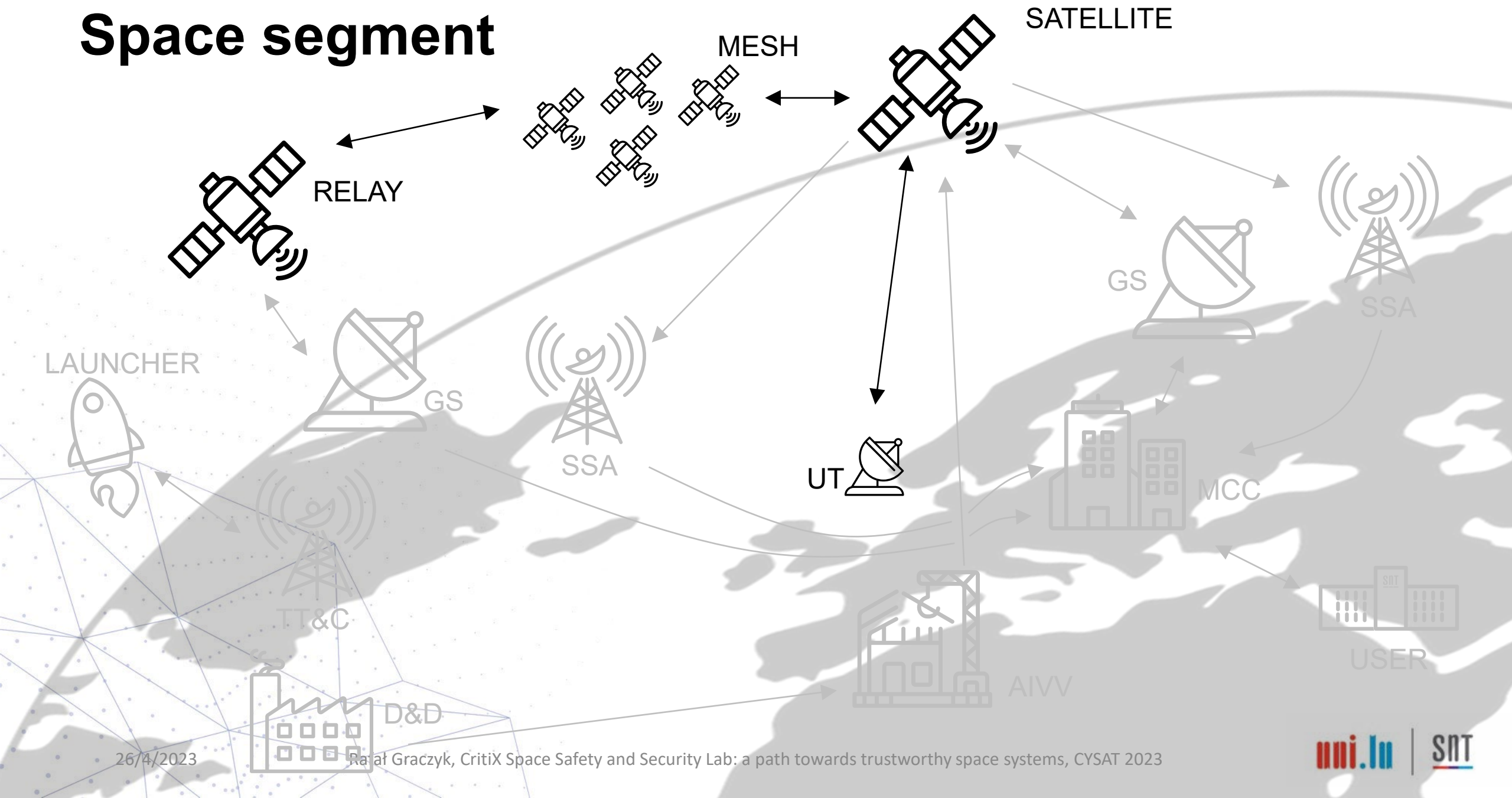
Launch segment



Attack Vectors – Launch segment

Loss of \ Affecting	launch operations
confidentiality	payload disclosure tracking
integrity	trajectory modification GNSS meaconing / spoofing
availability	loss of launcher no separation

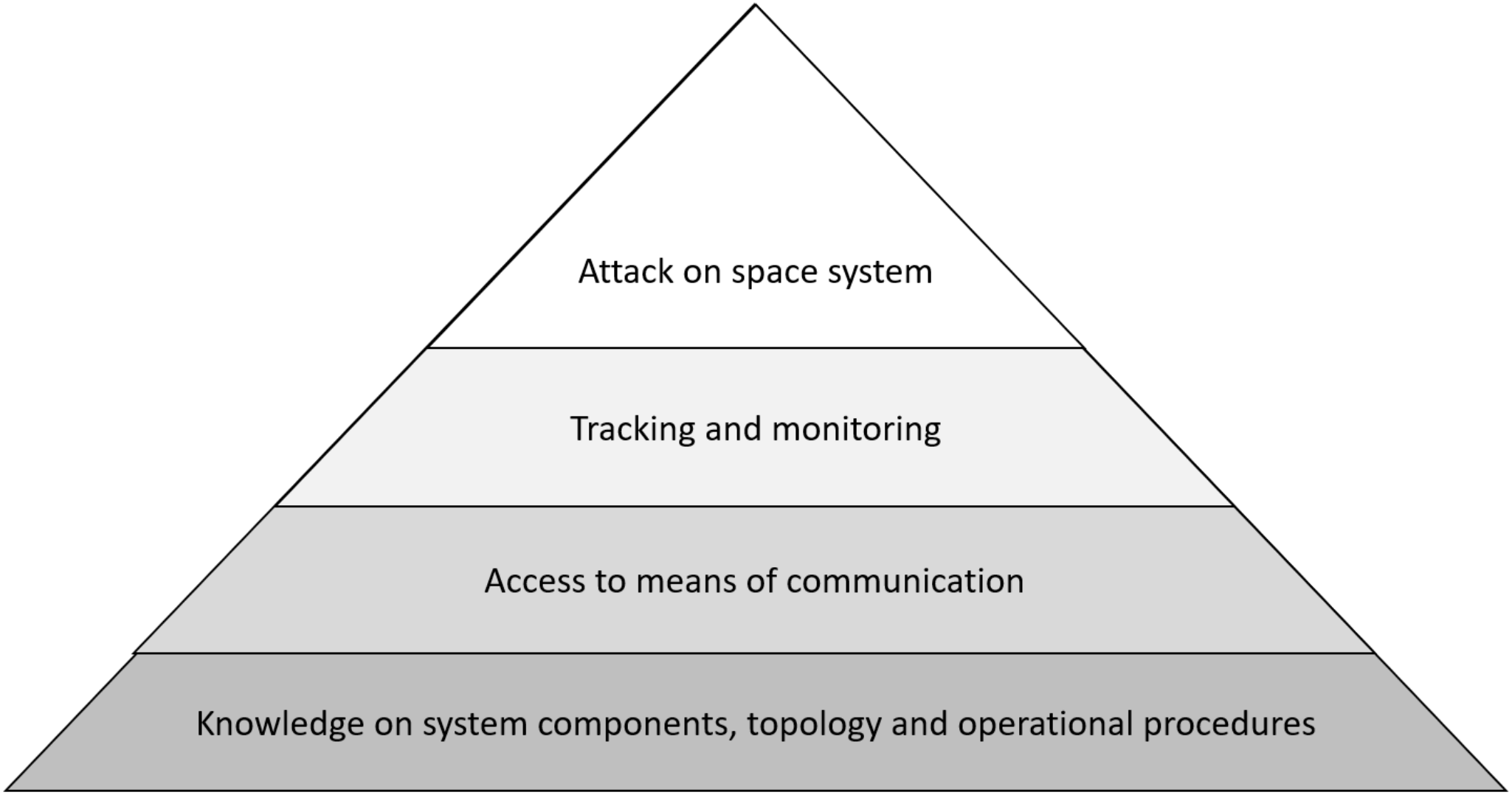
Space segment



Attack Vectors – Space segment

Loss of \ Affecting	satellite	mesh / relay	user terminal
confidentiality	unauthorised access	eavesdropping	eavesdropping tracking
integrity	unauthorised access and commanding fault induction	masquerading	data modification meaconing spoofing
availability	jamming blinding failure induction	denial of service jamming	jamming service disruption

Space system attack hierarchy




SNT
So… what now?
UNIVERSITY OF LUXEMBOURG

Let’s educate!

1. Red teams
    - what is there to attack?
    - what skillsets are required?
2. Blue team
    - how to monitor the assets and infrastructure?
    - how to ensure system availability?
3. Raise awareness
    - on criticality of space infrastructure
    - on risk factors and how to manage them

Let’s experiment!

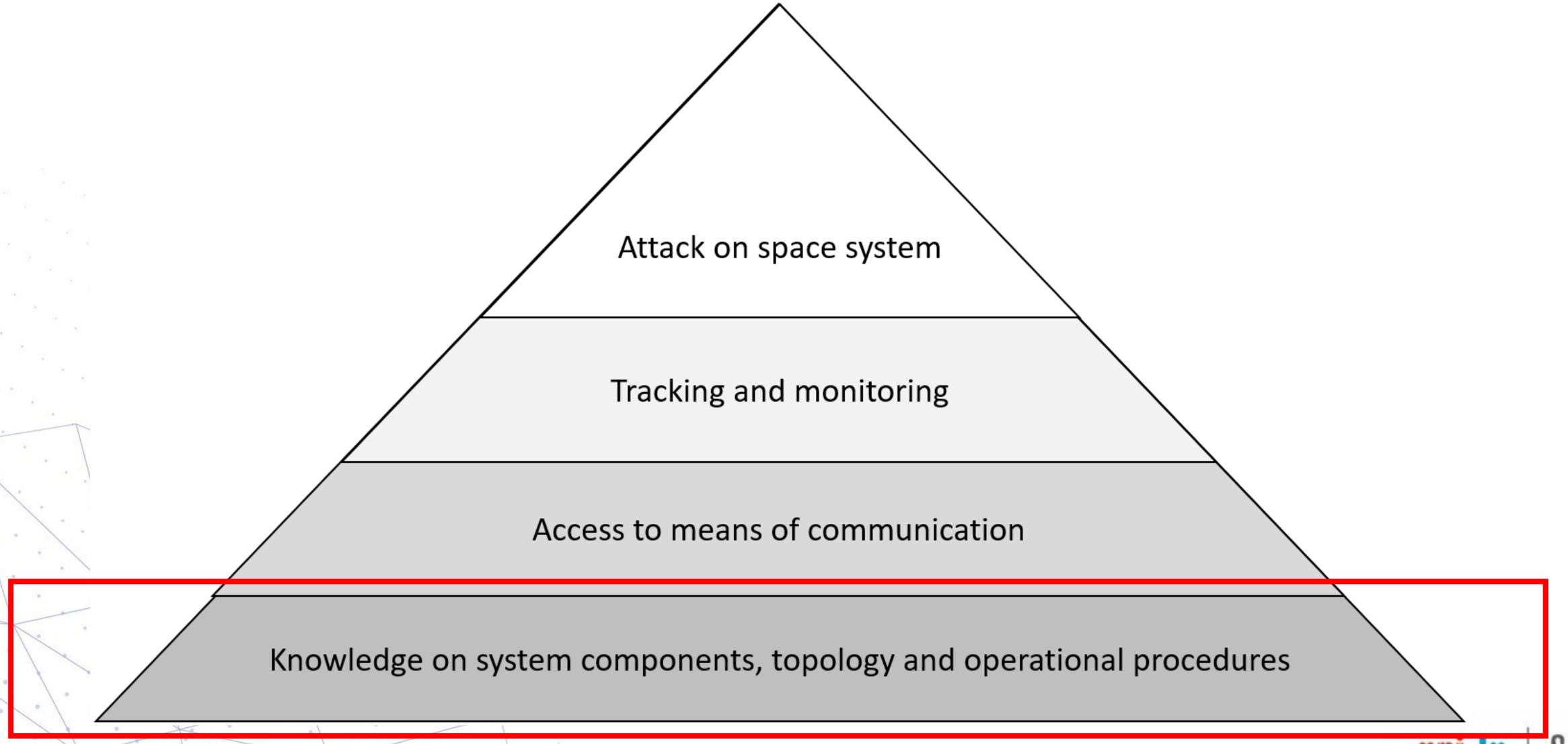
1. Search for vulnerabilities
    - open source HW/SW
    - standard interfaces
    - common building blocks
2. Develop resilience
    - experiment with fault and intrusion tolerance
    - in realistic set-up, with real-world limitations

SnT

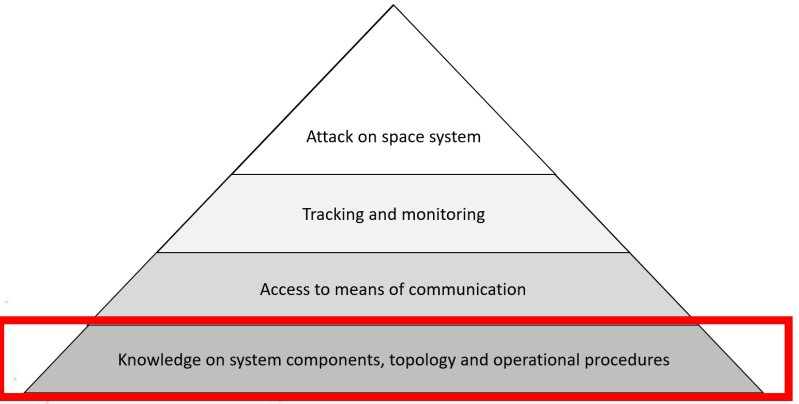
CritiX S^4 Lab

uni.lu
UNIVERSITY OF LUXEMBOURG

Mapping the space systems attacks - knowledge

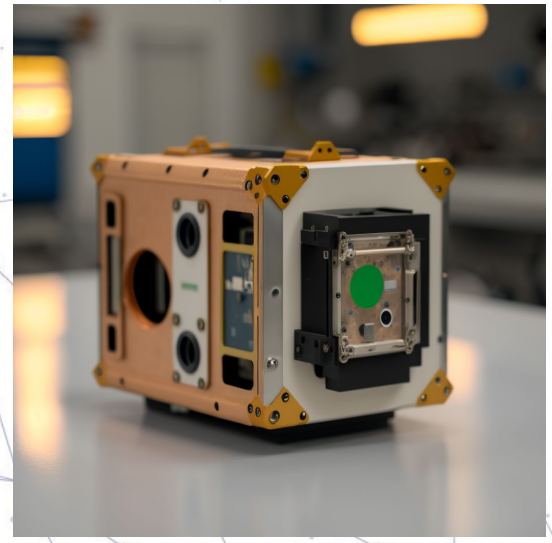


Mapping the space systems attacks - knowledge



CubeSat Design Specification
(1U – 12U)
REV 14.1
CP-CDS-R14.1

CUBESAT



libcsp / libcsp Public

Notifications Fork 213 Star 378

Code Issues 9 Pull requests 2 Actions Wiki Security Insights

develop 4 branches 8 tags Go to file Code

johandc Merge pull request #394 from pxntus/develop ... b2996d2 on Dec 4, 2022 1,793 commits

.github/workflows	github: Add FreeRTOS build test	2 years ago
contrib	examples/csp_server_client: Fix swapped prints	last year
doc	Typo fixes	5 months ago
examples	examples/csp_server_client: Fix swapped prints	last year
include/csp	Merge branch 'master' into develop	last year
src	cmake: interfaces: zmq: Fix setting PIC flag to a wrong target	8 months ago

About

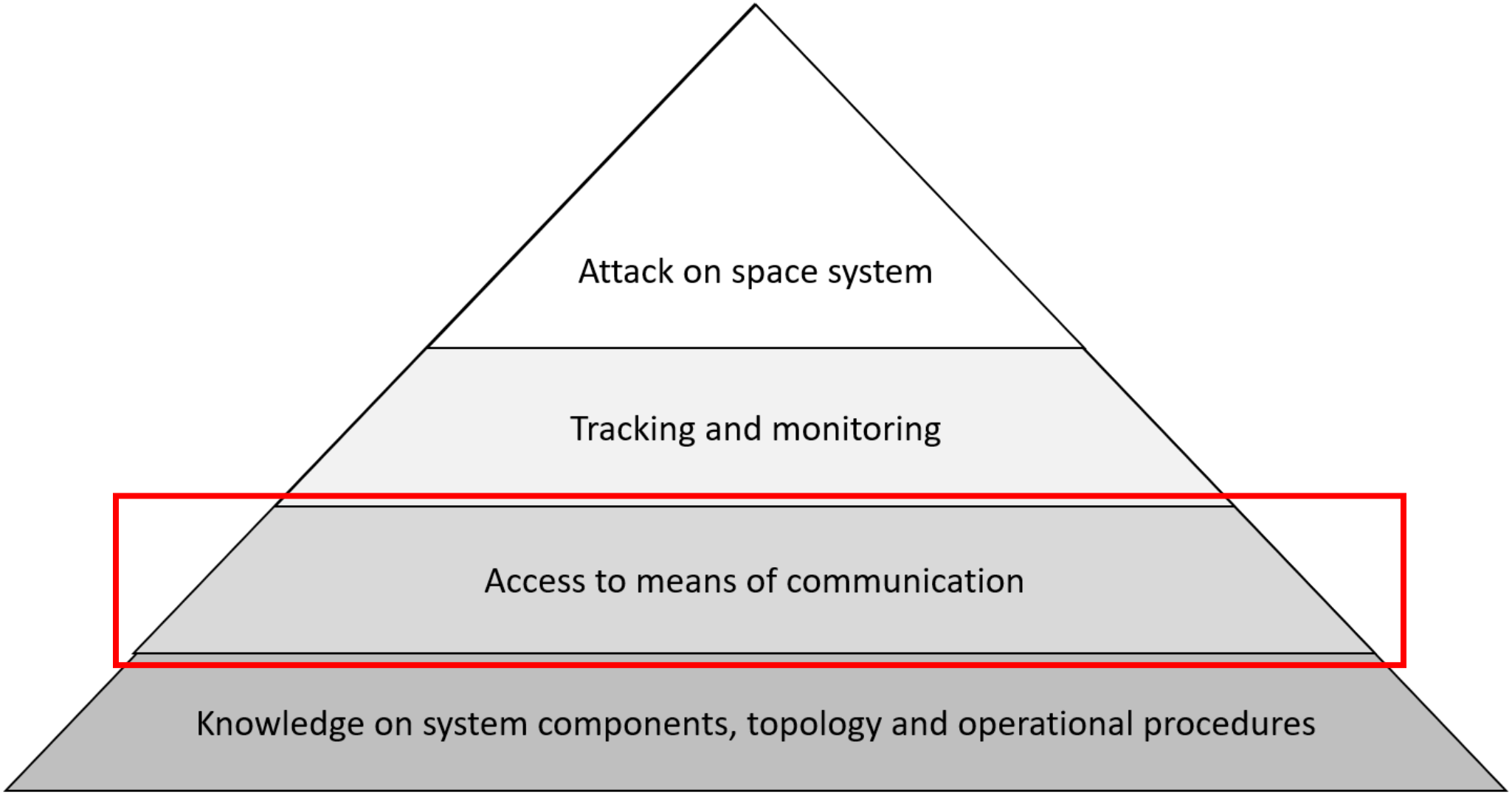
Cubesat Space Protocol - A small network-layer delivery protocol designed for Cubesats

www.libcsp.org

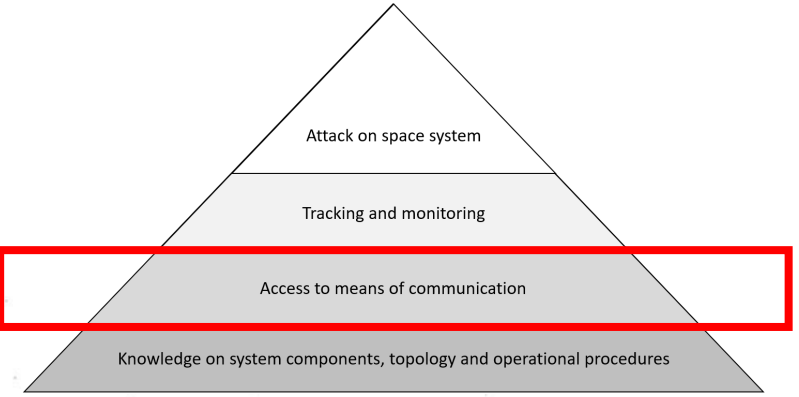
c protocol satellite cubesat

Readme
MIT license
378 stars
40 watching

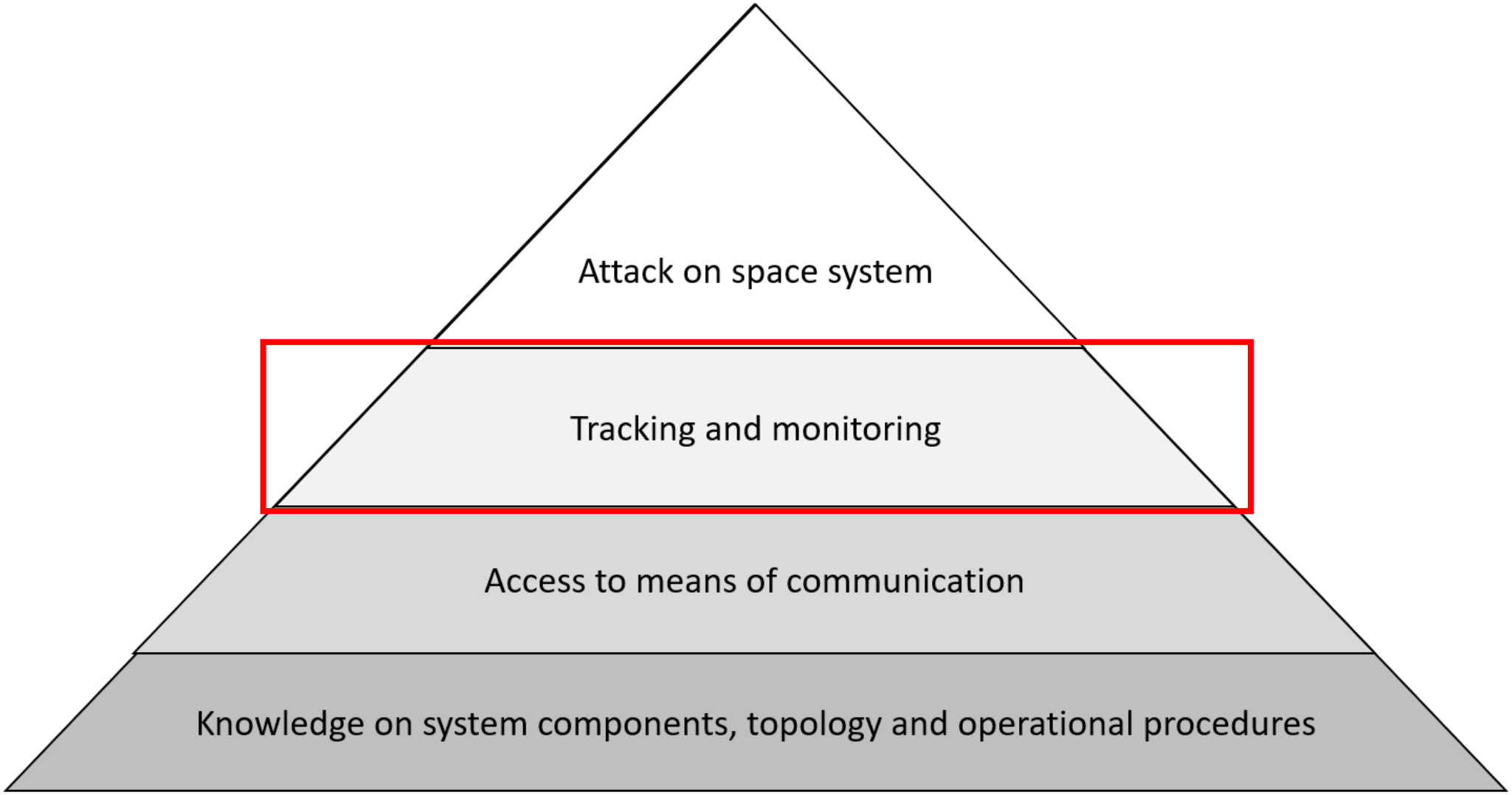
Mapping the space systems attacks - comms



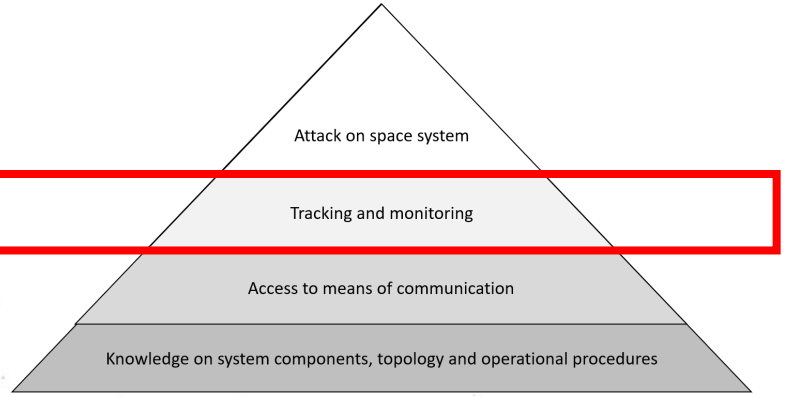
Mapping the space systems attacks - comms

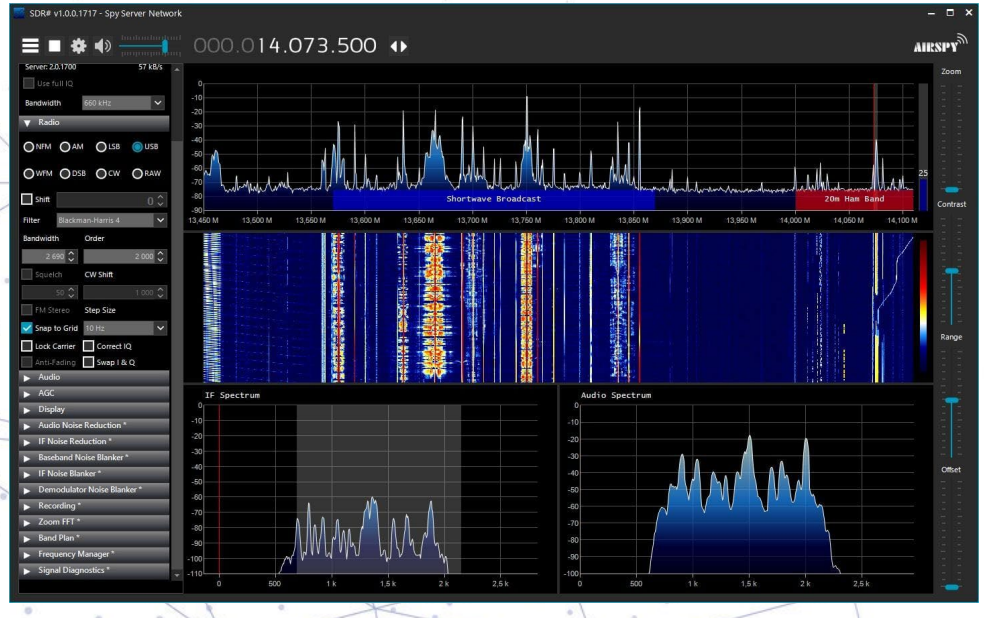


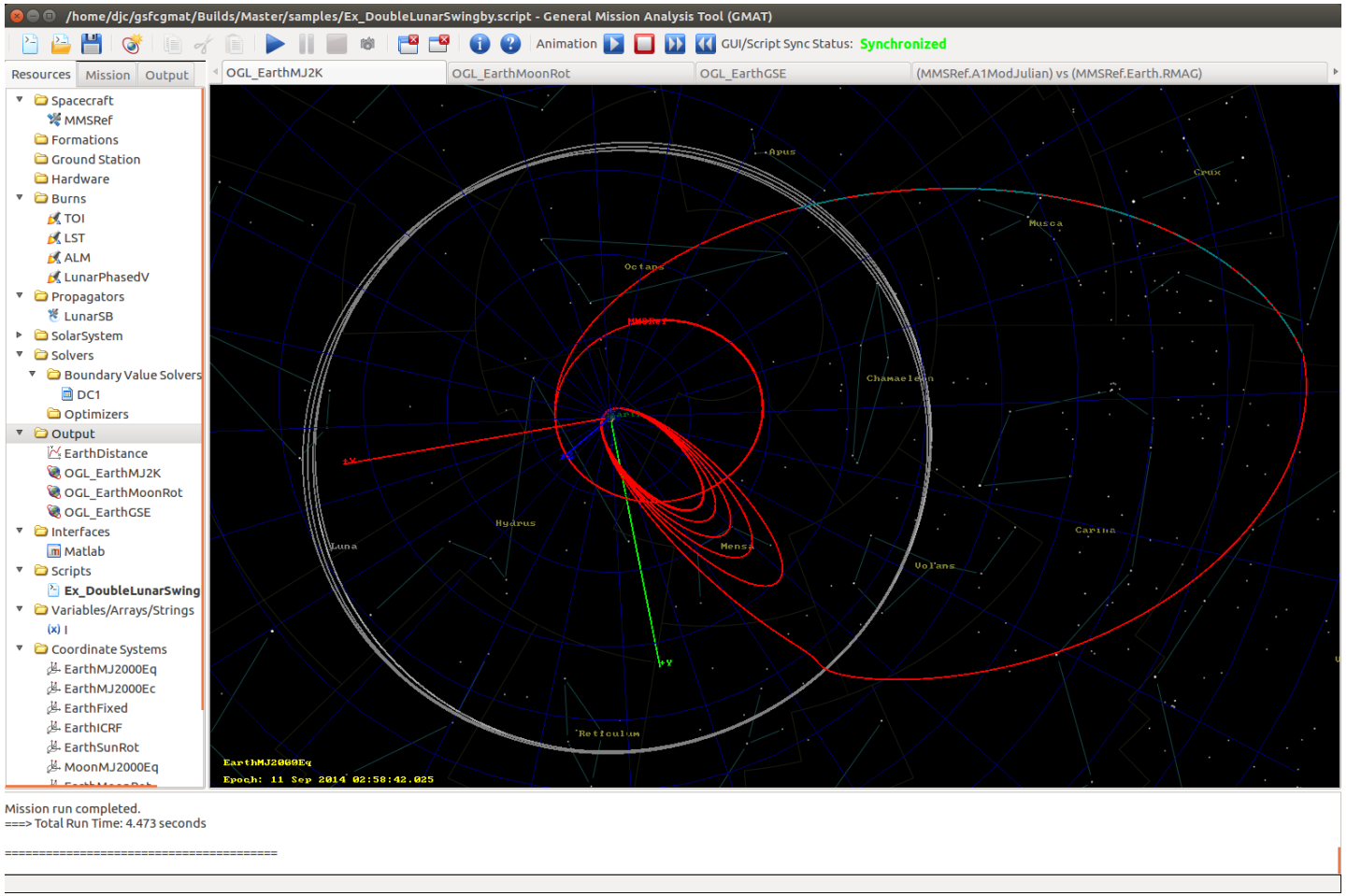
Mapping the space systems attacks – track & mon



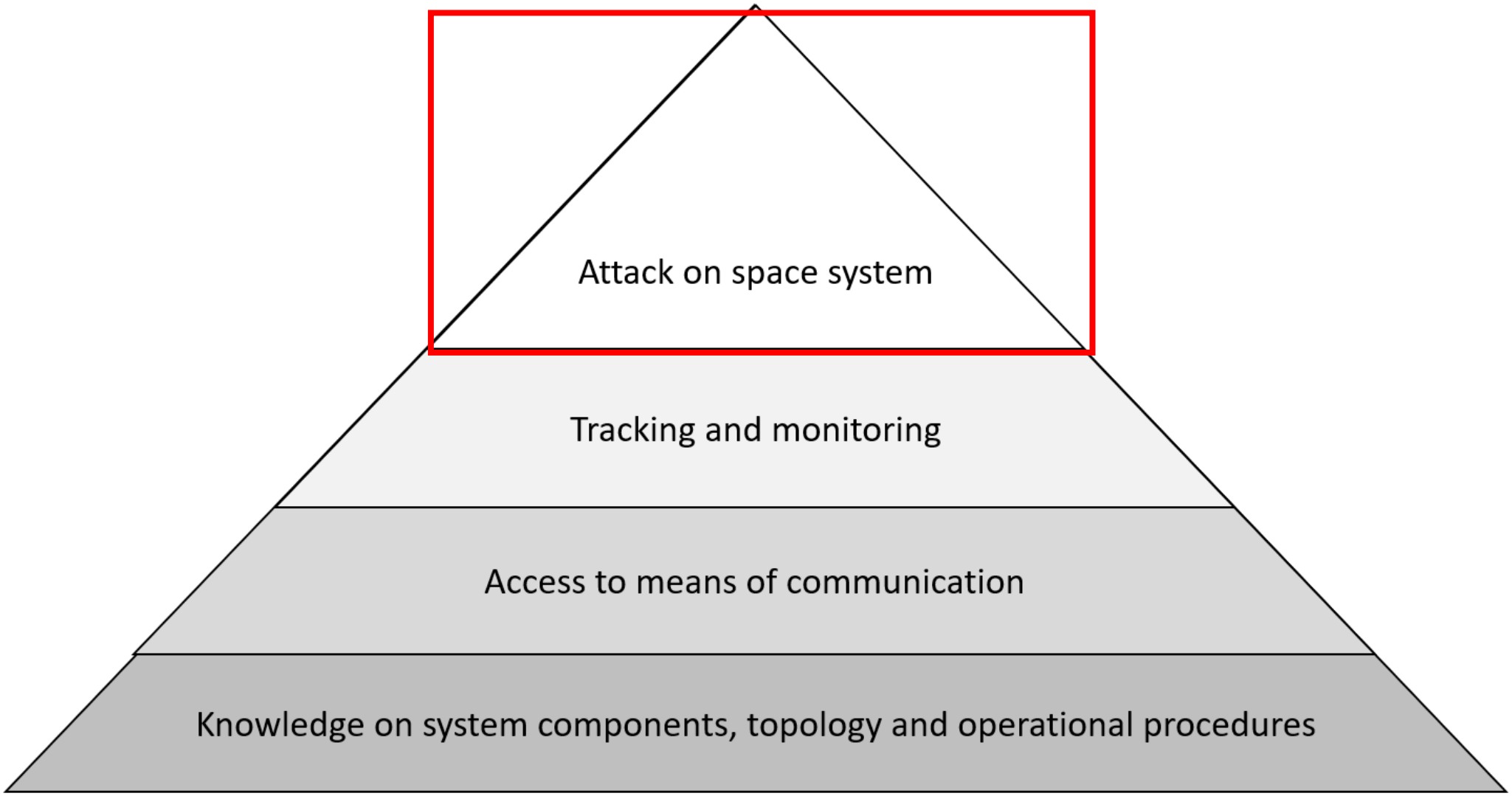
Mapping the space systems attacks – track & mon



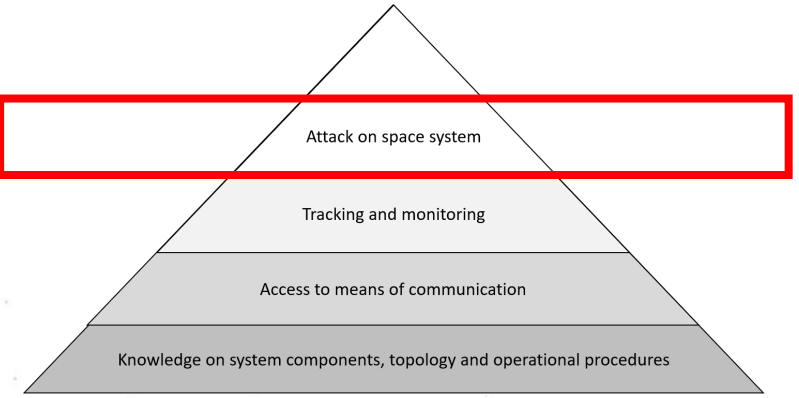


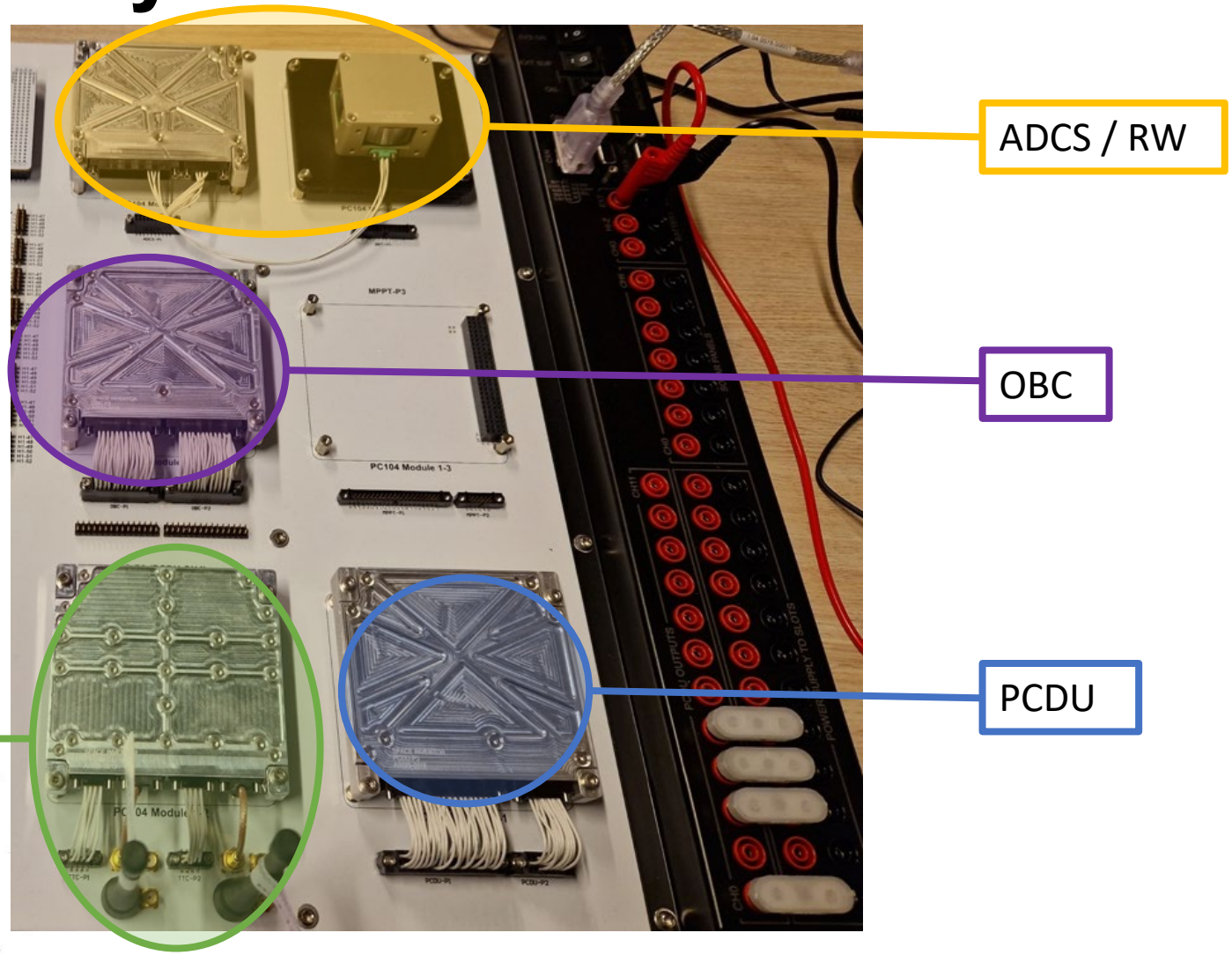


Mapping the space systems attacks – attack



Mapping the space systems attacks – attack





Concluding remarks

Building secure future for space infrastructure is a team work!

We’re open for collaboration:

- joint research
- partnership
- consultancy

Feel free to get in touch:
rafal@graczyk.io
rafal.graczyk@uni.lu

https://www.linkedin.com/in/rafalgraczyk/

Thank You!

CritiX Space Safety and Security Lab: a path towards trustworthy space systems

Rafał Graczyk