Switch_

# Behind the Shield: Tales from the Incident Frontline

25.09.2024

Darja-Anna Yurovsky

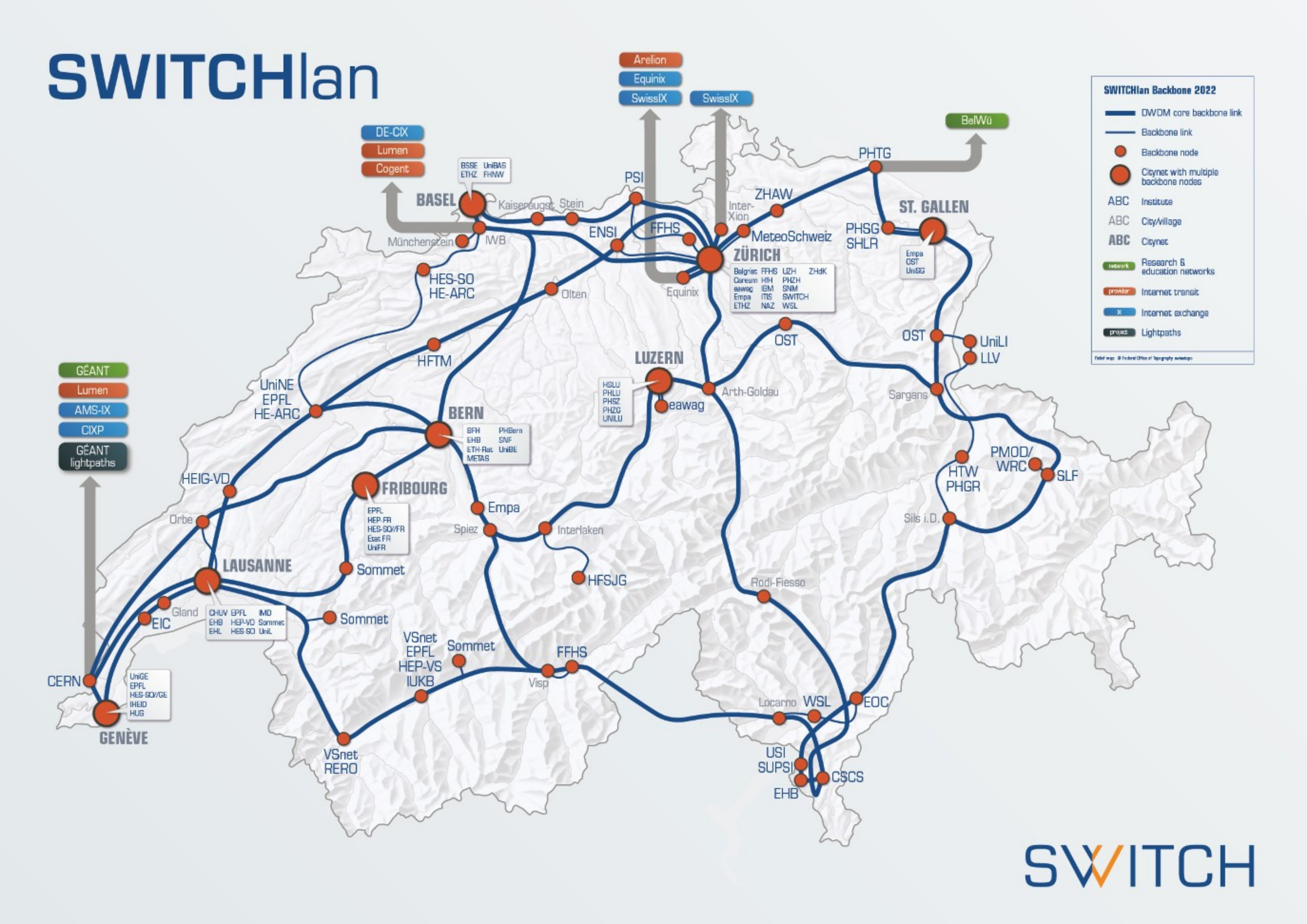
**TLP: AMBER**

# Agenda

# About Switch

> The foundation's objective is to create, promote and offer the necessary basis for the effective use of modern methods of telecomputing in teaching and research in Switzerland, and to support and be involved in such methods.
>
> It is a non-profit foundation that does not pursue commercial goals.

# NREN- National Research and Education Network



# Switch CERT

**We help our customers to protect their ICT infrastructure by...**

**trying to prevent incidents.**

**reducing the damage in the event of an attack.**

**coordinating countermeasures across our community.**

# What I am talking about…

**Security incident**

a security incident is an undesirable event that threatens operational safety and or disrupts operations

**Incident response**

Reactive response to ensure that violations/incident are effectively addressed, contained and restored to normal operation.

# Elements of an IT security incident

- […] Threat to your company
- Moment of surprise
- Rapid developments
- High degree of uncertainty
- Limited (and sometimes incorrect) information
- Short time to make decisions
- Pressure from external interest groups/media

# The Incident

An IT-security incident presents an interdisciplinary challenge, and collaboration across disciplines is the critical ingredient for success.

# whoami

Darja-Anna
Yurovsky

**Senior Security Engineer**
**MSc Digital Forensics, MA Data Science**
**@Switch since 2020**
**Experience in Incident Response, IT-Forensics, LE, Forensic Readiness, Security Advocacy etc.**

**darja-anna.yurovsky@switch.ch**

Switch_