High-level Research in Cybersecurity – Road to Competitiveness

Tomáš Pitner, tomp@fi.muni.cz

LAB OF SOFTWARE ARCHITECTURES
AND INFORMATION SYSTEMS

FACULTY OF INFORMATICS
MASARYK UNIVERSITY, BRNO

Cybersecurity Research Trends

- **Major Areas in Cybersecurity Research**
- **The European Quantum Communication Infrastructure (EuroQCI) Initiative**
- **Neighboring Areas**
  - **Sustainability**
  - **Energy Security**

lasaris

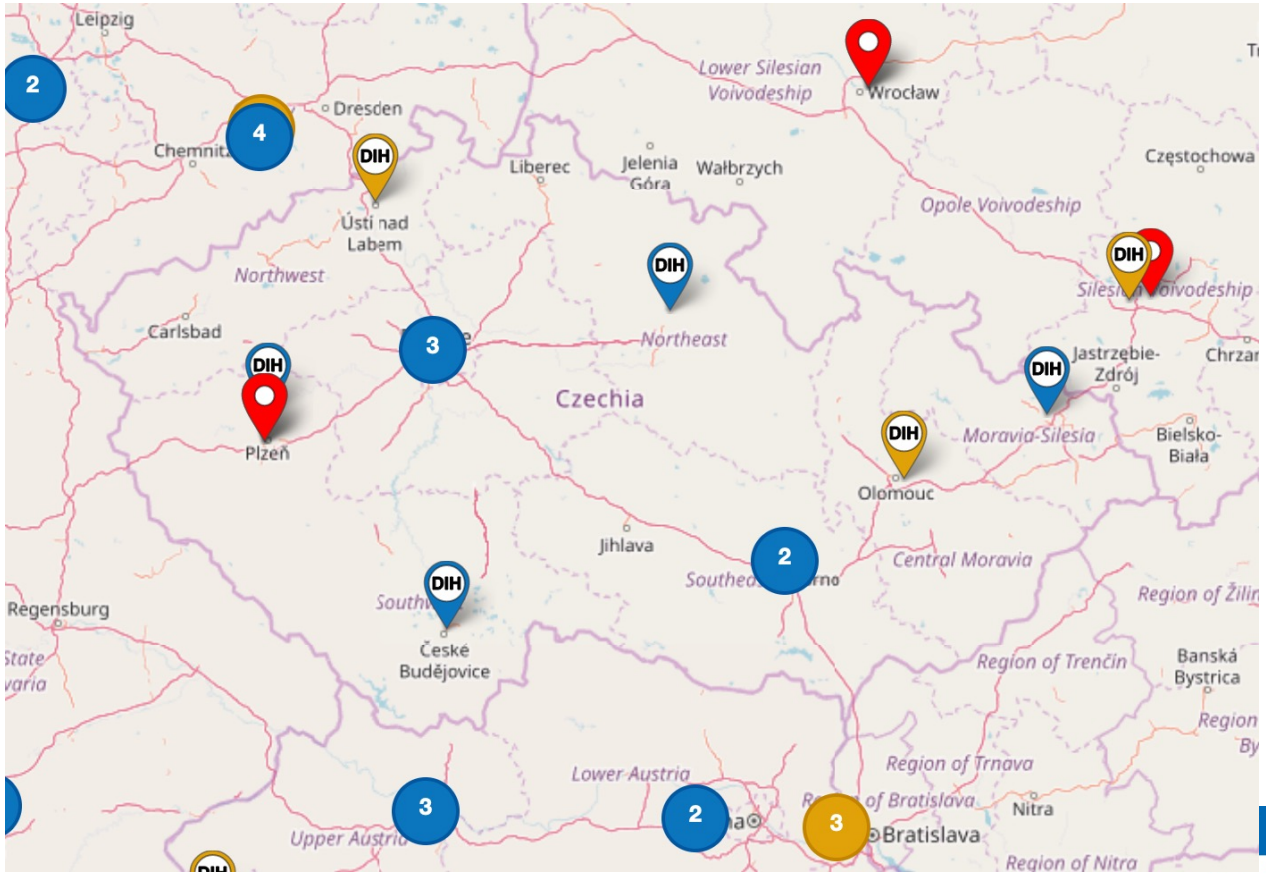
The Digital Europe Programme

- Digital Europe Programme (**DIGITAL**) is a new EU funding programme focused on
- bringing digital technology to **businesses**, **citizens** and **public administrations**.
- *Digital Europe Programme will reinforce EU critical digital capacities by focusing on the key areas of artificial intelligence (AI), cybersecurity, advanced computing, data infrastructure, governance and processing, the deployment of these technologies, and their best use for critical sectors like energy and environment, manufacturing, agriculture and health.*

lasaris

Digital Innovation Hubs

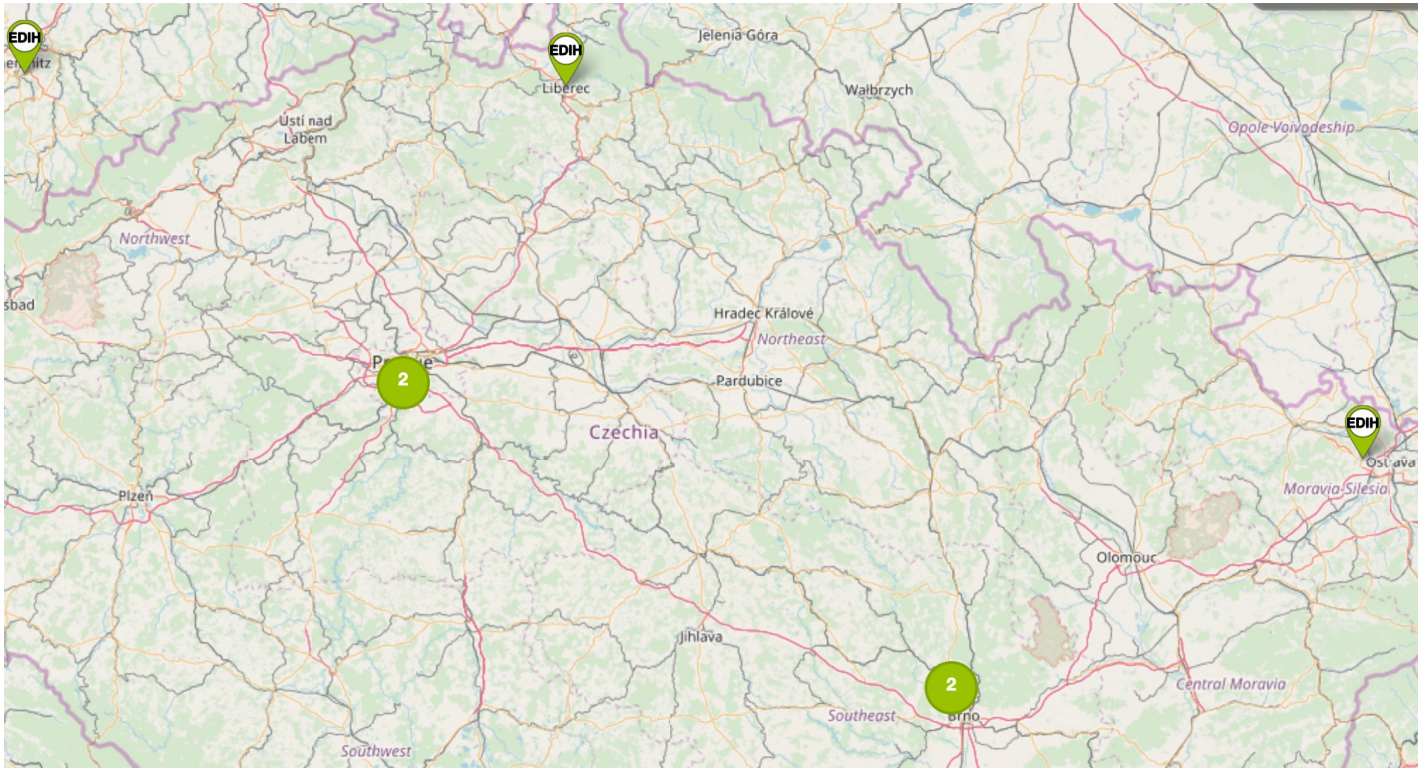
- „Centra digitálních inovací“



lasaris

European Digital Innovation Hubs

- „Evropská centra digitálních inovací“



lasaris

Digital Europe Programme's – Cybersecurity for 2021 - 2022

Security Operation Centres (SOC)

The creation, interconnection and strengthening of Security Operations Centres (SOC) can improve cybersecurity resilience with faster detection and response to cybersecurity incidents at national and EU level by leveraging disruptive technologies and sharing of information leading to increased situational awareness and stronger EU supply chains.

A key element will be capacity building, e.g. by leveraging artificial intelligence and dynamic learning of the threat landscape.

lasaris

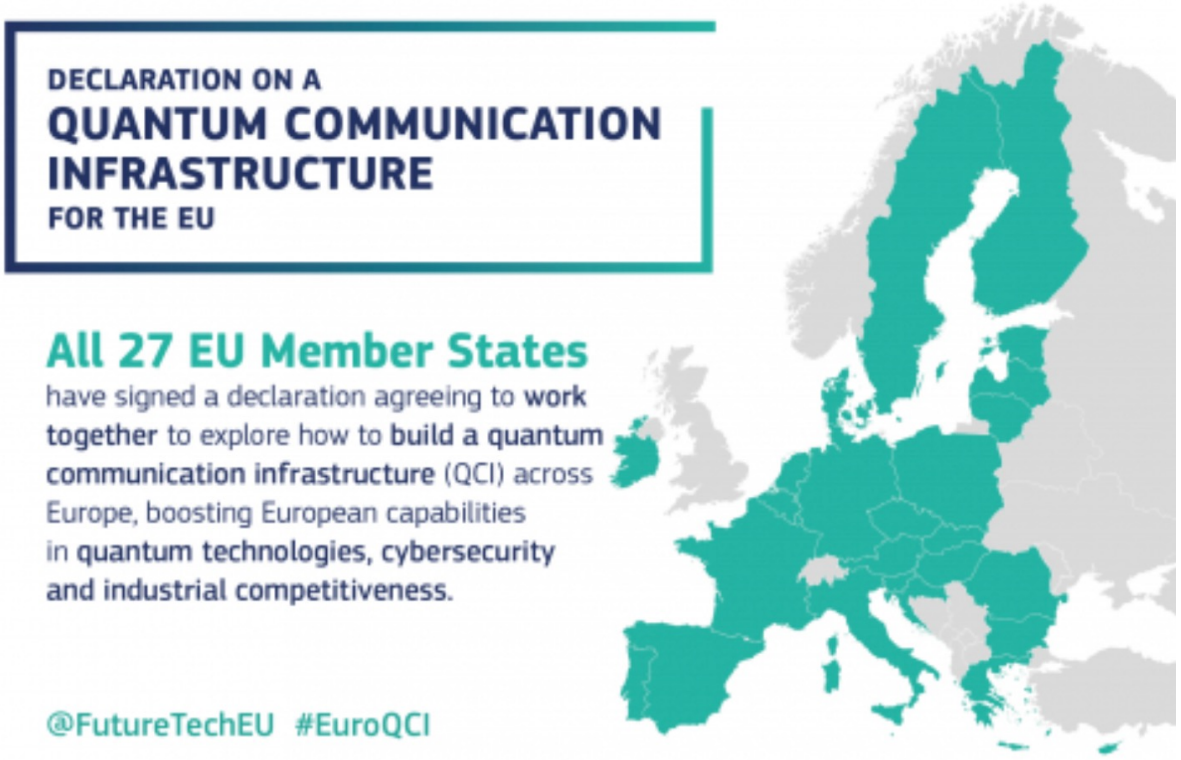
European Programmes

- Funding for the EuroQCI is being provided by the Digital Europe programme and the Connecting Europe Facility, as well as Horizon Europe, ESA, and national funds, including the Recovery and Resilience Facility.
- In 2021-2022, the **Digital Europe** programme will fund support for:
  - the **development of European QKD devices** and systems
  - the development and deployment of **national quantum communication networks**
  - a **testing and certification infrastructure** for QKD devices, technologies and systems that will ultimately be used in the EuroQCI.

lasaris

EuroQCI

- **EuroQCI** initiative aims to build a secure quantum communication infrastructure that will span the whole EU.



EuroQCI

- Serve to boost Europe's scientific and technological capabilities in cybersecurity and quantum technologies.
- improve Europe's digital **sovereignty** and industrial **competitiveness**.

lasaris

Global Cybersecurity Research Trends

- Selected research topics:
  - Machine learning (AI) in CS
  - Adaptive learning and training in CS
- Major domains:
  - Telco networks
  - **Power grids, microgrids**
  - E-health

lasaris

Cybersecurity of Microgrids

- **Microgrids** – small-scale, low, or medium voltage power systems with a decentralized group of electricity sources and loads
- **Smart Microgrids** (SM), we refer to microgrids that are based on networked control systems
- Commonly connected to outside to receive remote **commands** or allow **remote maintenance**.
- The used network may include **wireless channels**, and the grid can be geographically **dislocated,**
- some devices physically **reachable** and prone to **attacks**.

lasaris

Cybersecurity of Microgrids

- Moreover, the electrical grid is a **critical infrastructure**,
- Target of attackers with **huge technical and economical capacities.**
- **Cybersecurity** > fundamental issue to improve the resilience of microgrids.
- Control networks in Supervisory Control And Data Acquisition (**SCADA**)
- vulnerabilities are currently addressed by **IEC 62351**, which is a standard developed by WG15 of IEC TC57

lasaris

Cybersecurity of Microgrids

- Applications include:
- **Substation Automation**,
- **Advanced Metering Infrastructures**,
- **Phasor Measurement Units**,

- Benefit of **SDN** in **isolating** different traffic types/applications, **prioritizing** traffic, assuring **resilience** and fast failure **recovery**, and for the implementation of **virtual network slices**

lasaris

Techniques – **SDN**

- quick reset and reconfiguration of switches in order to isolate suspicious devices in the microgrid;
- establishment of application-specific filtering operations in the switches located close to attack sources; and
- on-demand path establishment for control commands to shrink attacker's operation time window.

lasaris

Techniques – **NIDS**

- **Network Intrusion Detection Systems** (NIDS) that analyze network traffic collected from one or more points of the communication network; and
- **Host Intrusion Detection Systems** (HIDS) that analyze the activity of a single host (i.e., a terminal) of the network.

lasaris

Techniques – **PADS**

- **Physics-based Anomaly Detection Systems** find many applications in the smart microgrid environment.
- After the development a consensus-based distributed voltage control architecture of isolated DC microgrids, an analytical consistency-based **anomaly detection mechanism**.

lasaris

Thanks for your attention!

- **Tomáš Pitner**, Room C218
- E-mail: pitner@muni.cz
- Phone: +420-778884996

lasaris