



**MASARYK  
UNIVERSITY**

Czech Republic

# **R&D and education in cybersecurity and critical information infrastructures**

**Tomáš Pitner**

**Masaryk University  
Brno, Czechia**



# Cybersecurity @MU at a Glance

- In context of **Security Studies**
  - (Geo)Political and Strategic
  - **Organizational, Technological, and Law**
- **C4e** as cooperative multidisciplinary research and education centre of Masaryk University
  - Cybercrime and cyber security
  - Protection of critical infrastructures
  - Law



# STRUCTURE

## Main Teams

- **CSIRT-MU – Institute of Computer Science MU**
- **Lasaris, Paradise, CroCS – Faculty of Informatics MU**
- **Institute of Law and Technology – Faculty of Law MU**
- **Institute of Politology – Faculty of Social Science**
  
- *and ad-hoc cooperation*

## CSIRT-MU

- **Computer Security Incident Response Team** of Masaryk University
- Part of the Institute of Computer Science
- Accredited by **Trusted Introducer**
- Long term experience with R&D in the field of network security monitoring
- [csirt.muni.cz](https://csirt.muni.cz)





# Lasaris

- **Lab of Software Architectures and Information Systems**
- Focus on the **protection of critical information infrastructures**
- Development of **resilient architectures** of IT systems
- [www.lasaris.cz](http://www.lasaris.cz)



## CroCS

- Centre for **R**esearch on **C**ryptography and **S**ecurity
- Aim to improve **security** and **privacy** through applied research
- cooperation with **industry**
- advanced **education** of future security professionals.
- [crocs.fi.muni.cz](http://crocs.fi.muni.cz)



## Institute of Law and Technology

- Focus on **technology law** (ICT law, data protection, intellectual property law, **energy law**, etc.)
- Long term cooperation with public authorities
- Expertise in the area of cybercrime & cyber security
- [cyber.law.muni.cz](http://cyber.law.muni.cz)







## What do we do?

- **Research and Development**
- Cooperation
- **Education**

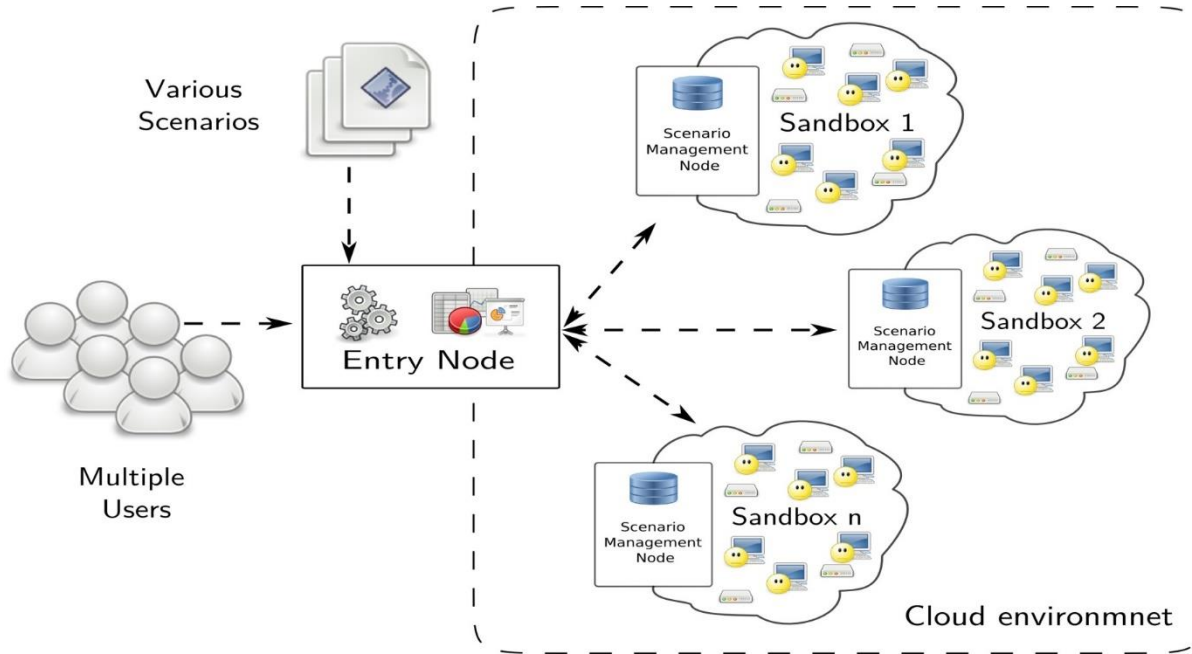


# RESEARCH INFRASTRUCTURE

## Cyber Range (KYPO)

- Unique cloud-based virtualized infrastructure environment developed by CSIRT-MU
- 3 main use-cases:
  - **Research**
  - Digital forensics (analysis and simulations)
  - **Cybersecurity trainings & exercises**
  - Further extension to **cyber-physical** world

# KYPO architecture





# KYPO Lab





# RESEARCH AREAS

## Types of Research

- **Strategic**
  - Cyber warfare, cyber terrorism, intelligence services
- **Technical**
  - Detection tools, information sharing tools, training platforms, forensic tools, **resilient IT systems and infrastructures**
- **Legal**
  - Cybercrime, cybersecurity & cyber defense law, data protection, ICT law, IP law, sectoral **regulation of critical infrastructures**
- Focus of the research is discussed at the meeting of the **rector's expert advisory board.**

## Selected Research Projects

- **KYPO**
- SABU
- SENTER
- LIVE\_FOR
- CRUSOE
- Experimental research of user behavior in ICT security
- **Smart metering**





# **EXAMPLE RESEARCH AREA – CRITICAL INFRASTRUCTURE IN POWER GRIDS**

## Smart Metering Research Areas of C4e

According to classification given by prof. Andrea Tonello:

- S1: Communication and Networking
- S2: Cybersecurity and Privacy
- S3: Control and Operation of Responsive Grids
- S4: Smart Metering, Demand Response and Dynamic Pricing
- S5: Big Data
- S6: Field trials, Standardization, Regulations

# S1: Communication and Networking

- **Reviews and surveys** (ČEZ, ČSRES),
- Reflection of **international experience**
- **Communication technology** for SM and SG:
  - Conception
  - **Planning** (new fibre optic lines) – for ČEZ
  - In-lab and in-field testing – for ČEZ
  - Regulations on telecommunications, energy business, cybersecurity, privacy, and critical infrastructure protection



## S2: Cybersecurity and Privacy

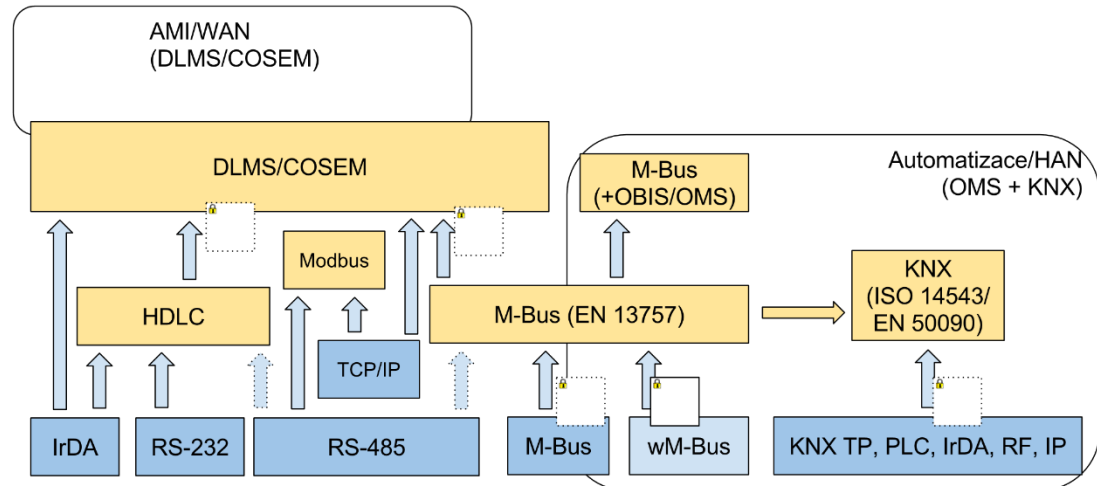
- Joint research projects for ČSRES (Union of Regulated Energy Businesses in CZ)
- Annual **National Cybersecurity Technical Trainings** (CyberCzech)
- In-lab **security testing** (eg. impact of security measures on performance)
- Further extension of our **KyPo Cyber Range** to cyber-physical systems

## S3: Control and Operation of Responsive Grids

- Joint research projects for ČEZ
- **Modeling**
- **Simulations**
- **Predictions** (of consumption, of metering behavior)
- **Control:**
  - Led by MycroftMind (Masaryk University spin-off) for ČEZ:
  - Project on **Local Optimization of Distribution Grid (LODIS)**

# S4: Smart Metering, Demand Response and Dynamic Pricing

- Design of the **Smart-meter**  $\leftrightarrow$  **Home Area Network** interfacing





## S5: Big Data

- Large computing and storage infrastructure available
- **CERIT Scientific Cloud**
- Both **data-intensive** and **computation-intensive** applications in smart grids based on deep learning

## S6: Field trials, Standardization, Regulations

- **Smart-grid lab** for ČEZ
- Conception of **lab control system**
- Both **HW** and **SW** part design and implementation
- Test control system driven by Design of Experiments (DoE),
- Inspired by **SW testing standards**, applied to **cyber-physical** systems
- Expertise in **Regulations** on Telecommunications, Energy business, **Cybersecurity, Privacy**, and Critical Infrastructure Protection

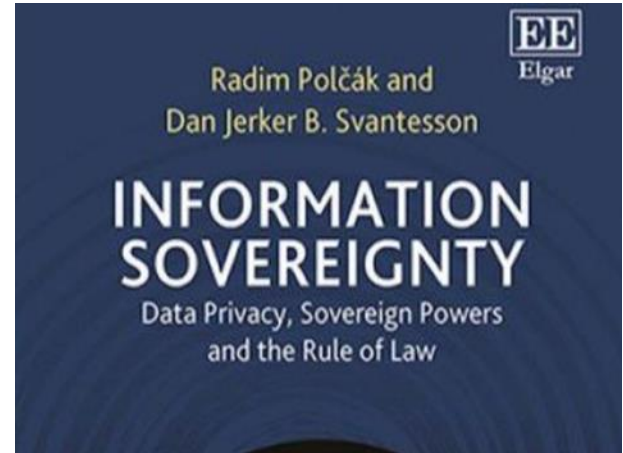




# INSTITUTIONAL COLLABORATION

# International cooperation

- **Europol (EC3)**
  - taxonomy of cyber security incidents,
  - lectures for LEA
  - expert boards membership
- **ENISA**
  - taxonomy
  - sharing of knowledge, expert boards membership
- **NATO**
  - taxonomy,
  - study programs (Cyber Defense Master), exercises (CCDCOE)





**TF-CSIRT**  
Trusted Introducer

---

## International cooperation

- **UN**
  - sharing of tools and knowledge
  - UNCITRAL and UNODC academic delegations
- **TF-CSIRT**
  - sharing of tools, knowledge, best practices, etc.
- **National research and education** institutions
  - ad-hoc cooperation, research projects, sharing of knowledge and tools



## National cooperation

- **National Cyber and Information Security Agency**
  - sharing of knowledge and tools
  - training and education: courses and exercises (Cyber Czech)
  - attendance at exercises: Locked Shields, Cyber Europe, EDA
- **Police**
  - sharing of knowledge and tools, consulting
  - training and education – cooperation with Police academy
- **Army and Ministry of Defense**
  - consulting and research focused on cyber defense tools

## National cooperation

- **Intelligence services**
  - consulting
- **Ministry of Interior**
  - research and development projects (KYPO, SABU – sharing of cybersecurity events data)
- **Ministry of Justice**
  - expert board on digital evidence
- **Judicial academy**, Public prosecutors office, Judges
  - training and education, consulting





## Other activities

- **CyberCon**
  - spring conference on cybersecurity
  - started as an initiative by FSS students in 2014
  - now organized primarily by NCISA
- **Multinational Cyber Defense** Education and Training Project
- **International Security** Summer School



# INDUSTRY

## CERIT Science Park

- Center for **E**ducation, **R**esearch and **I**nnovation in **ICT**
- Size (22.238 sq ft, capacity ~20 companies)
- Focus of companies:
  - **Modeling and simulation of critical infrastructures**
  - **Computer network security**
  - **Infrastructure monitoring**
  - High-performance multimedia processing
  - Development of systems for data processing
  - Visualization and graphic services
  - Web applications, analysis and marketing
  - **Mobile security solutions**
  - Open source systems







## Association of Industrial Partners

- Goal: long-term collaboration
- Dominant indicators so far (\*required)
- Financial contribution\* (mostly for students, equipment)
- Student involvement\* (# of graduation thesis)
- Collaborative R&D
- PhD sponsoring (required at strategic level)



# Technology transfer

- (Central) Technology Transfer Office at MU
- Framework: regulations, PR, IP management, legal services
- Support at origin of research results
- ICT as integrated pillar covering:
  - Faculty of Informatics
  - Institute of Computer Science
  - Science Park
  - Institute Law and Technology (Faculty of Law)
  - other units with ICT interests





# EDUCATION



## Education – Faculty of Informatics

- 3-year Bachelor program in **Informatics**
- 2-year Master program in **IT Security** (technology) and **Cybersecurity management**
- 4-year Doctoral program in Computer Systems and Technology, research areas of **Cybersecurity** and **Critical Infrastructure Protection**



## Education – Faculty of Social Sciences

- 3-year Bachelor program in **Security Studies**
- 2-year Master program in **Security Studies**
- new 2-year Master program **Conflict and Democracy Studies**
  - taught in English
- both include courses on cybersecurity, information warfare, propaganda, hybrid conflicts, and emergent threats

## Education – Faculty of Law

- Lectures and trainings
  - **Judicial** and **police academy** (cybercrime investigation, digital evidence handling, intellectual property, data protection)
  - Ad-hoc **trainings** (for investigators, experts, public prosecutors)
  - **KYPO** hands-on training and exercises (sysadmins, CSIRT members)
- Bachelor degree (**ICT security**) – in cooperation with University of technology
- Masters degree (**Cyber security – interdisciplinary and law**)
- **Doctoral** study program



## Education – international

- **Joint doctoral degree** – with University of Haifa
- Masters study programs **NATO (Multinational Cyber Defense Education and Training Project)**
- Ad-hoc courses and trainings – NATO

## Education - regular events

- Seminars:
  - iSysel
  - Cyber cake
- Conferences
  - Cyberspace ([cyberspace.muni.cz](http://cyberspace.muni.cz))
  - Czech law and information technology ([cpit.law.muni.cz](http://cpit.law.muni.cz))
  - Energy Law Symposium
- Summer school on ICT law





# FURTHER DEVELOPMENT

## Strengths

- Benefit from presence at **University**
- **Complex** view from strategic and legal to technical aspects, from theoretical to applied
- Unique ability to react to complex **problems**
- Top **international team** and **collaboration**
- Unique **infrastructure** (**KyPo**, Science Park, Cloud)
- Based on strong **research** (**C4e** and many labs)



# Opportunities

- Extension of study programmes
  - **Doctoral** studies
  - **Master** programmes (cybersec **management**)
  - **Professional** programmes (experts for daily operations)
  - **Lifelong** learning programmes
  - Study programmes in **international networks**