MUNI

Cybersecurity and Resilience in Energy Sector and other Critical Infrastructures

Tomáš Pitner, Lasaris Head
pitner@muni.cz
https://www.linkedin.com/in/tomaspitner/

Cybersecurity and Resilience

- **CS and Resilience** as key challenges today
- **Lasaris** CS research in context of @FI and MU
- Roots in **trust** and **reliability**
- Always **holistic** view incl. law and regulations, geopolitics, ethical values and principles, business view

MUNI

Cybersecurity and Resilience

- **Cybersecurity** refers to the **practices, technologies,** and **processes** designed to protect computers, networks, programs, and data from attack, damage, or unauthorized access.
- It encompasses a range of measures taken to safeguard **digital information** and **assets** against cyber threats, such as **malware, phishing, and hacking**, ensuring the **integrity**, **confidentiality**, and **availability** of information.

- **Resilience** refers to the ability of an individual, community, system, or material to **withstand, adapt to**, and **recover from stress, challenges,** or **adversity**.
- It embodies the capacity to bounce back from difficult situations, maintaining functionality, or even emerging stronger.
- In **psychology**, resilience is often discussed in the context of mental health and coping mechanisms. In materials science, it describes the capability of a substance to return to its original shape after deformation.
- Across contexts, resilience highlights **strength, flexibility,** and **adaptability** in the face of obstacles.

MUNI

Cybersecurity and Resilience
Same or different research communities?

Alessandro Gabrielli — Počet citací tohoto článku: 175317
Associate Professor, Physics and Astronomy Department (DIFA), University of Bologna
E-mailová adresa ověřena na: unibo.it
General Physics Microelectronics Firmware Design Trigger and DAQ for HEPE Cybersecurity

Federico CALZOLARI — Počet citací tohoto článku: 138562
Scuola Normale Superiore, CERN, INFN
E-mailová adresa ověřena na: sns.it
Computer Science HPC Big Data CyberSecurity Particle Physics

Distinguished Prof. Athanasios Vasilakos — Počet citací tohoto článku: 69825
UiA,Norway
E-mailová adresa ověřena na: uia.no
AI IoTs Networks-6G-Big Data Analytics Cybersecurity Applied Crypto and Network Se…

Alexander Bentley-Sutherland — Počet citací tohoto článku: 63402
Professor of Cybersecurity, University of Edinburgh
E-mailová adresa ověřena na: hipaadigital.com
Cybersecurity HIPAA Healthcare

Carlos Filipe Da Silva Costa — Počet citací tohoto článku: 40936
Previously at the University of Florida
E-mailová adresa ověřena na: cern.ch
physics High energy gravitational waves Cybersecurity Cyberdiplomacy

Alan R. Dennis — Počet citací tohoto článku: 37036
Professor and John T. Chambers Chair of Internet Systems, Indiana University
E-mailová adresa ověřena na: indiana.edu
Information Systems digital humans Fake News cybersecurity collaboration

Carl Folke — Počet citací tohoto článku: 236797
Beijer Institute, KVA, Stockholm Resilience Centre, Stockholm University, Sweden
E-mailová adresa ověřena na: beijer.kva.se
social-ecological systems resilience ecological economics sustainability science global change

dennis charney — Počet citací tohoto článku: 187825
icahn schoold of medicine at mount sinai
E-mailová adresa ověřena na: mssm.edu
psychiatry mood disorders anxiety disorders resilience

Wei Wang — Počet citací tohoto článku: 174656
Tongji University
E-mailová adresa ověřena na: tongji.edu.cn
Steel Structure Seismic Engineering Ductile Fracture Resilience Progressive Collapse

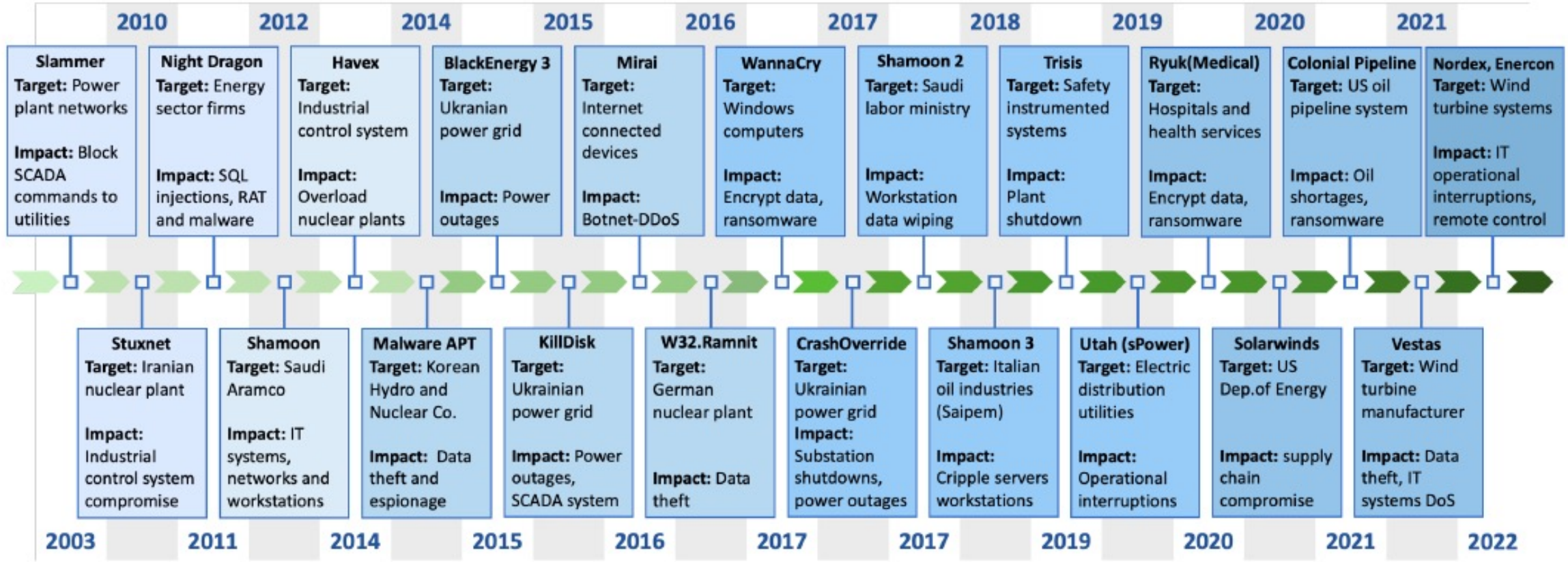
Neil Adger — Počet citací tohoto článku: 140890
Professor, Geography, College Life and Environmental Sciences, University of Exeter
E-mailová adresa ověřena na: exeter.ac.uk
Sustainability resilience ecological economics human geography climate change

Brian Walker — Počet citací tohoto článku: 137442
Research Fellow, CSIRO Australia
E-mailová adresa ověřena na: csiro.au
Ecology resilience complex systems

Ann S. Masten — Počet citací tohoto článku: 102131
Regents Professor, Institute of Child Development, University of Minnesota Twin Cities
E-mailová adresa ověřena na: umn.edu
resilience competence development disaster war

MUNI

Reality is only one:
Significant Attacks against Energy Infrastructure



Source: Zografopoulos et al. (2023) **Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations** arXiv:2205.11171v4

MUNI

The view of the attacker as a necessary aspect

- A comprehensive cybersecurity solution must include
- the adversary view that can not only mitigate against
- previous "what happened" incidents, but also
- actively defend against "what could happen" scenarios.

- The same problem as with democracy:
- we are right but cannot use all instruments the attackers can

MUNI

Multidomain attacks must be defended by multidomain readiness and response

- Supply-chain resilience
- Critical resources
- Technology autonomy
- Strategic planning
- Robust regulation
- Regional/EU and overseas partnership
- De-globalization
- Environmental, social and corporate governance (ESG)
- Insurance policy
- Credit policy (banks)
- Subsidy policy (governments)
- Tax policy (governments)
- (complete) Openness policy

MUNI

Domain examples & our R&D+E interests

- **Cybersecurity**
- **Cyber range**
- Forensics & f. readiness
- **CS Education**

- **Energy supply and delivery**
- **Flexibility** in supply/demand
- Energy communities
- CS in transmission and distribution

- **Semiconductors**
- Chip design
- Supply chain
- Position of CZ in Europe
- **ACDRC** in CZ/Brno

- **Cyber-physical systems**
- Introduction to IoT
- IoT/ICS Security

MUNI

Energy supply and delivery: good example of complex approach needed

- **Vulnerability analysis**
- Entire supply chain
- Case of electricity: direct impact on other CI

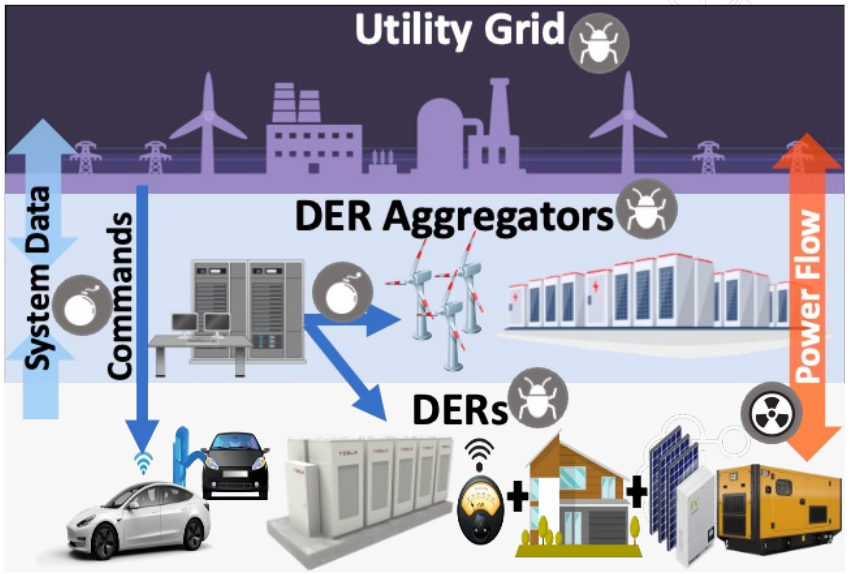
- **Importance of IT and OT sec**
- Both are vital: you cannot produce if you cannot sell

- **Regulations**
- Scope: more than single nation

- **Business aspects**
- Just about (private) profit vs loss?
- Externalities

MUNI

Distributed power supplies expand the security perimeter



Vulnerabilities	Attacks	Impacts	Mitigations
Lack of encryption and authentication	Network reconnaissance	Disruption of grid operation	Secure communication protocols
Unauthorized network expansion/joins	MAC spoofing/flooding	Frequency and voltage instabilities	Authentication and authorization schemes
Insecure communication	Data eavesdropping and Packet replay	Power quality degradation	Network whitelisting, traffic monitoring and IDS/IPS systems
Remote access/control	Control command tampering	DER generation, availability and control malfunction	Secure firmware updates
Unsigned firmware updates	Denial-of-Service		

MUNI

Attacks against DER - scenarios studied

Disruptions in DER

- Random outages
- Natural phenomena
- Deliberate attacks

MUNI

Attacks against DER - possibility or reality?

Cyber-attacks that target Demand-Response in smart grids by injecting false information about **consumption** and **generation**

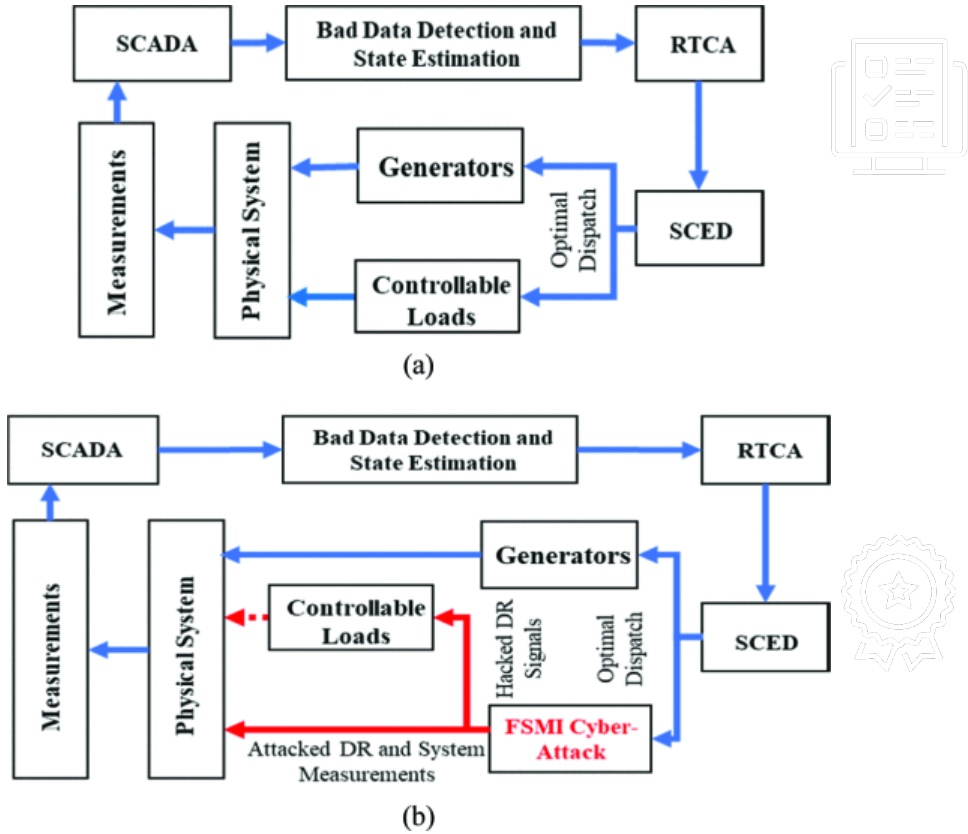
Possibility such of attack experimentally verified:

Increase the **load** on the distribution network by 8-28%

Increase the cost (finance) of **ancillary services**

MUNI

The principle of attacks against DER



Source: Daogui Tang et al. (2023) **Vulnerability analysis of demand-response with renewable energy integration in smart grids to cyber attacks and online detection methods.**
Reliability Engineering and System Safety, Elsevier.

MUNI

Experiments with attacks and defences

Cyber attacks against DR in smart grids by injecting fraudulent consumption and production information

Countermeasures: online detector based on convolutional neural networks

Detect cyber attacks + mitigate their impact

Works against attacks with fixed rates of change,

Attacks with variable rates of change are in principle difficult to detect

Attack vectors and potential threats

Poor interoperability

Cause: diversity and inconsistency in architecture and implementation specifications (e.g. security requirements) can lead to insecure communication between systems

Consequence: rejection of legitimate messages and commands for DER

Source: Zografopoulos et al. (2023) **Distributed Energy Resources Cybersecurity Outlook: Vulnerabilities, Attacks, Impacts, and Mitigations** arXiv:2205.11171v4

MUNI

Attack vectors and potential threats

Data integrity breaches

Stored, transmitted or received data is **modified without authentication**,

Consequences: causes DER **failures** or allows **unauthorized access** to control/logging information.

Threat: Malicious modification of control parameters

MUNI

Attack vectors and potential threats


Implementation vulnerabilities

Security flaws in systems and/or communication modules allow remote control of active DER elements and exfiltration of historical data

Threat: Potential for unauthorized production/load control

MUNI

Attack vectors and potential threats

Compromised supply chain

Possible installation of spyware malware residing on hardware, worms, oversights in manufacturing of components, equipment or systems

Threat: Exposure of sensitive information

MUNI

Attack vectors and potential threats

Insecure firmware

Digital signatures of firmware updates are not authenticated, allowing malware (viruses, worms, Trojans, etc.) access to secure systems

Threat: Escalation of permissions on DER systems

MUNI

Attacks in hierarchical management systems

- autonomous systems
- distributed hierarchical control architectures
- many entry points for an attacker
- possible cascading effects


MUNI

Summary of the main sources of vulnerabilities

- Smart grid systems face many vulnerabilities due to their interconnected nature, multitude of devices and communication networks
- Lack of interoperability and standardisation
- Systems consist of disparate components from different manufacturers
- Using different communication protocols
- Physical security risks (unauthorised access, tampering, physical attacks)
- Inconsistent regulatory and policy frameworks across jurisdictions
- How to implement uniform security measures and share information

MUNI

What we do for safety

- Cybersecurity Innovation Hub - SMEs, public sector
- Concentration of know-how across the Czech Republic
- Czech part of EU Quantum Communication Infrastructure
- National Cybersecurity Coordination Center NCCC

In-house cybersecurity know-how

13 years of connecting practice, research and education

Mentoring and guiding other universities in the field of cyber security.

We have created an open-source platform for cybersecurity training.

1st cybersecurity team certified by Trusted Introducer in the Czech Republic

MUNI

Our story

- Supported by the Ministry of the Interior of the Czech Republic
- First open-source Cyber Range in the EU
- Introduction of open format training and exercises
- Used for exercises for banks and the energy industry

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

REWIRE
CYBERSECURITY SKILLS ALLIANCE

WARWICK
THE UNIVERSITY OF WARWICK

SIEMENS

Ministry of Defence
Czech Republic

eg·d

ČEPS

ČESKÁ SPOŘITELNA

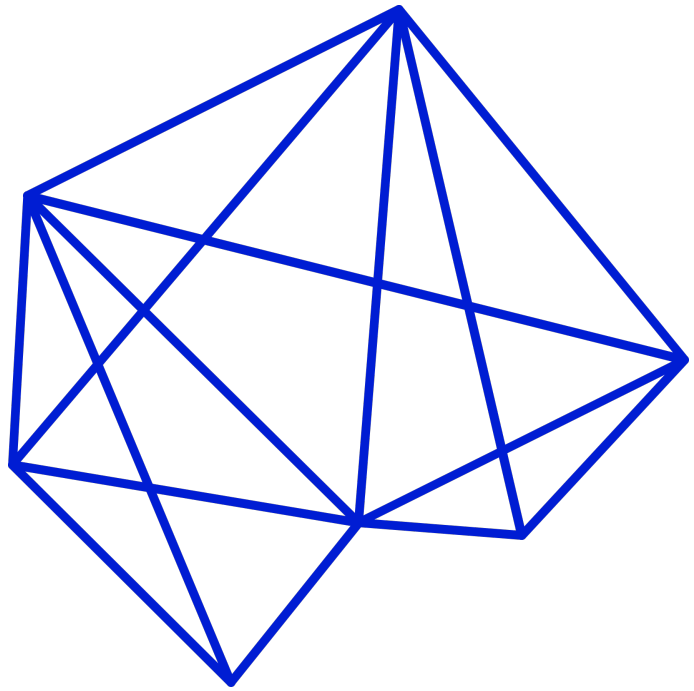
Support for national coordination centres

- National Contact Points aim to promote research and competitiveness
- KYPO offers itself as an EU platform for education.
- We have started negotiations with neighbouring countrie
- We try to provide other services.

MUNI

Cyber Range open source and open content

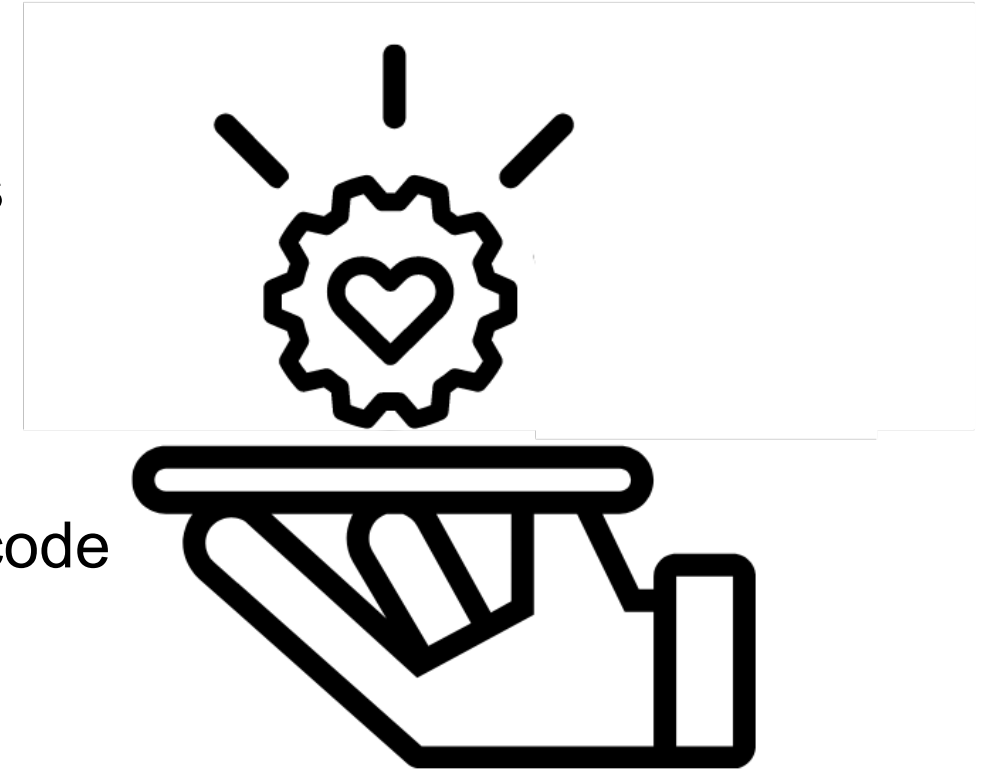
- Initiative to provide open alternatives to commercial.
- 10 confirmed deployments.
- KYPO and content is available for free.
- We are looking for more users and support.



MUNI

Benefits of open training and exercise

- Human and machine readable format
- Interchangeable between KYPO CRP instances
- Possibility to transfer to other domains
- Use of widely accepted tools
- Adheres to the principles of infrastructure as a code
- High level of code reusability



MUNI

Use cases

Training

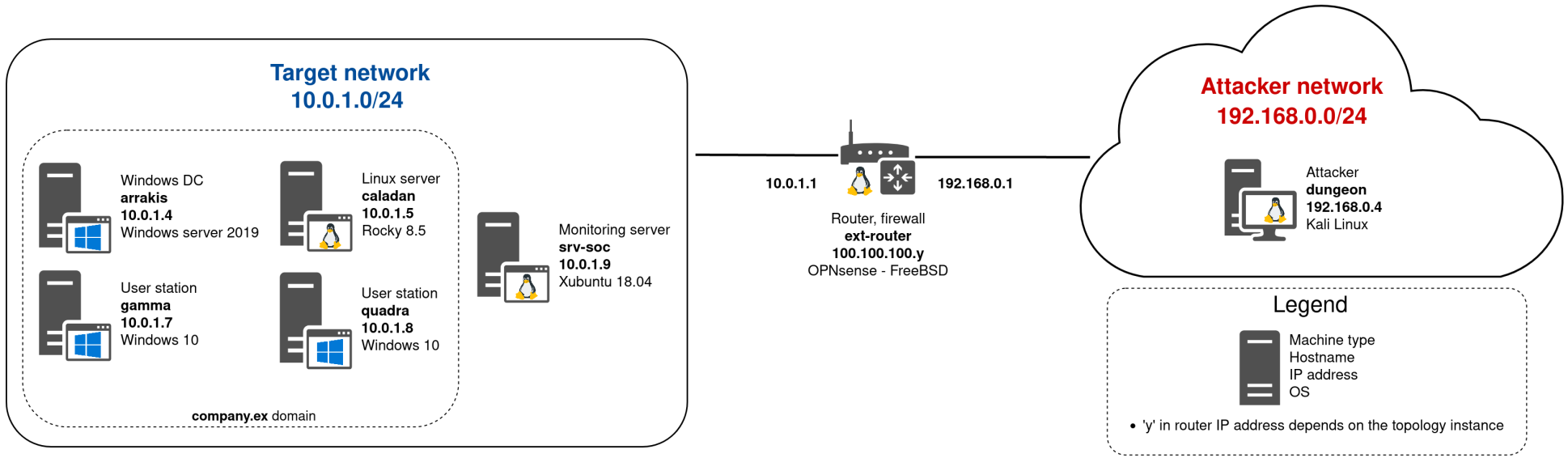
- Practical training similar to CTF
- Practical action by **the red** or **blue** team
- Focused on improving skills
- Free training content is available

Exercise

- Realistic exercises
- Focused on **red/blue** team activities
- Multidomain event
- Available as a service

MUNI

Training



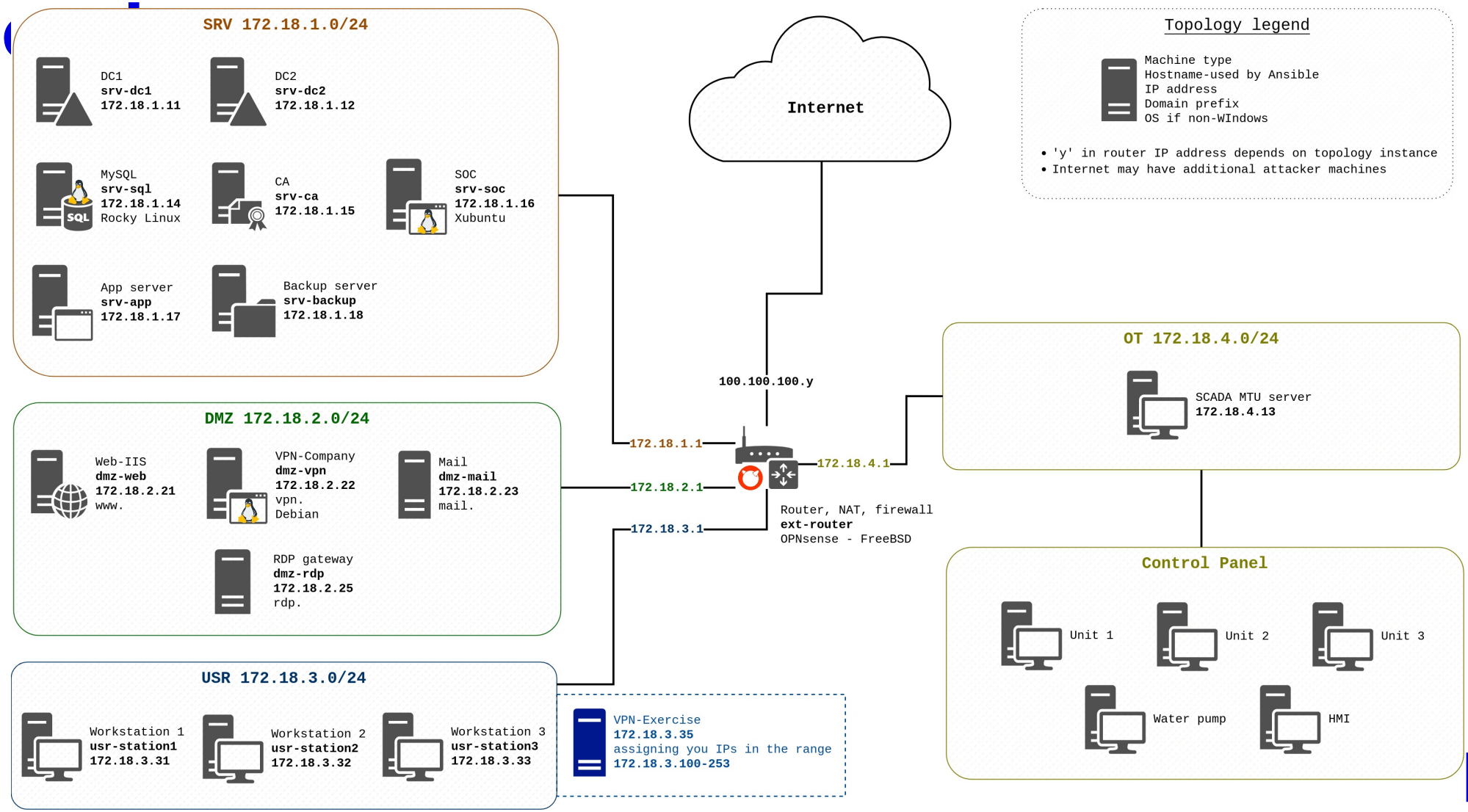
MUNI

Commercial Cyber Security Exercise

- The activity is based on the CyberCzech exercise (with NUCIB).
- We have established a long-term cooperation with ČEZ.
- We plan to expand into other sectors.
- The exercises focus on practical experience.
- Exercises track current Advanced Persistent Threats and attacks.
- We provide realistic tools, procedures and attacks.

MUNI

Exercise - IT training environment in the cl



MUNI

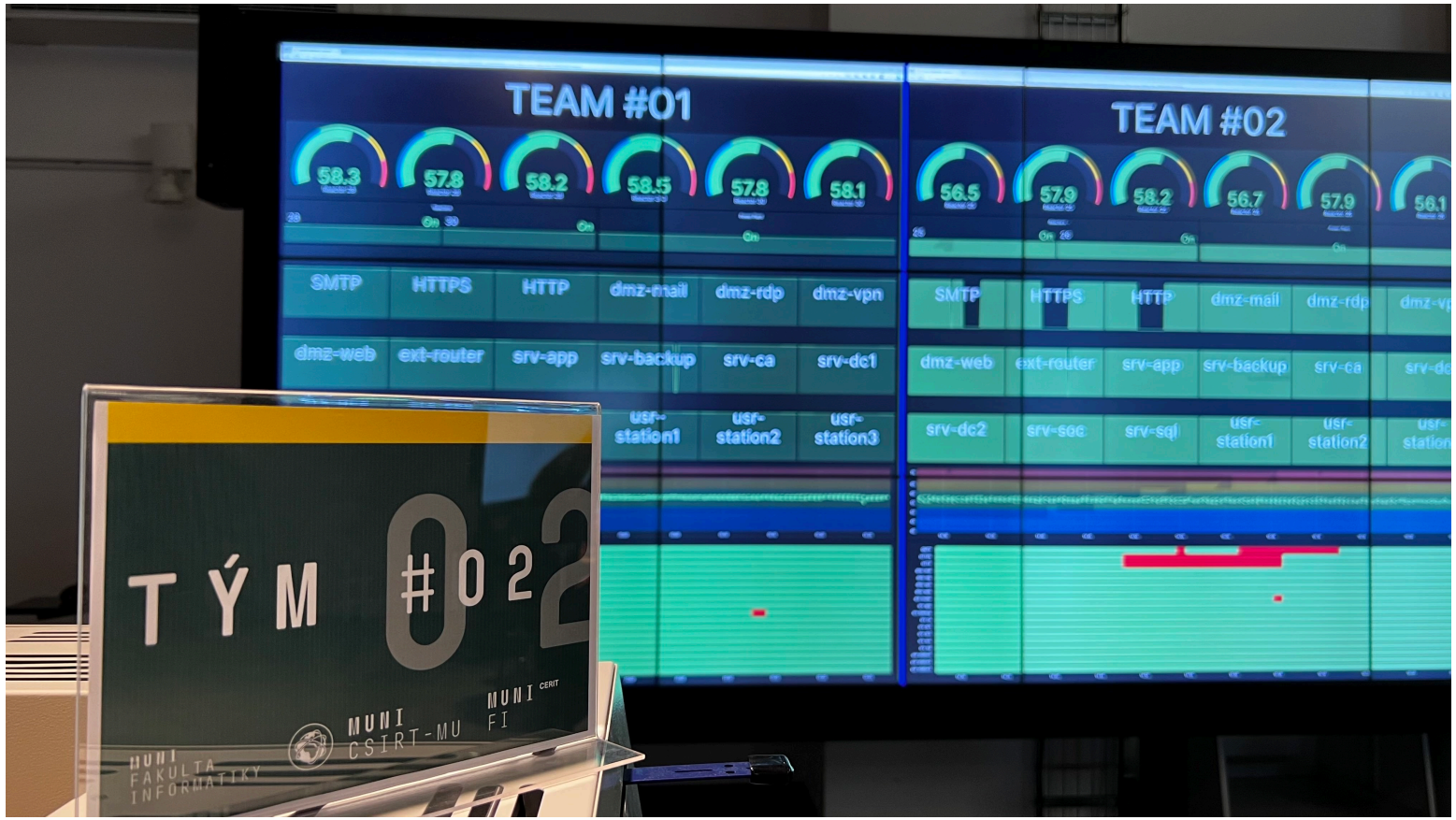
Exercises - OT systems

MUNI

Exercise - "Situational Awareness"

MUNI

Exercise - team tracking



MUNI

Our vision

Everyone can become part of a growing community.

Open content and support tools are available.

The development is being guided by the KYPO CRP Steering Committee.

A practical training platform for the ECCC and ENISA.

MUNI

KYPO CRP Related links

- **KYPO Cyber Range Platform** crp.kypo.muni.cz
- **Documentation** KYPO CRP docs.crp.kypo.muni.cz
- **Cyber** training **and training** services.kypo.muni.cz
- Official **Twitter account** @kypocrp

MUNI