RESEARCH CHALLENGES AND STRATEGIC PROJECTS IN CYBERSECURITY

Tomas Pitner, Head of Lasaris

CYBERSECURITY HUB – RATIONALE

- Cybersecurity Hub, z. ú. (CS HUB) was founded in 2020 by three Czech universities:
  - Masaryk University
  - Czech Technical University in Prague
  - Brno University of Technology

- Goals:
  - Development of cooperation and initiatives in the field of cybersecurity and related technological areas,
  - Development of joint initiatives in the field of certification services for cybersecurity
  - Supporting the digital transformation of companies, especially SMEs and public administration organisations in the field of cybersecurity.

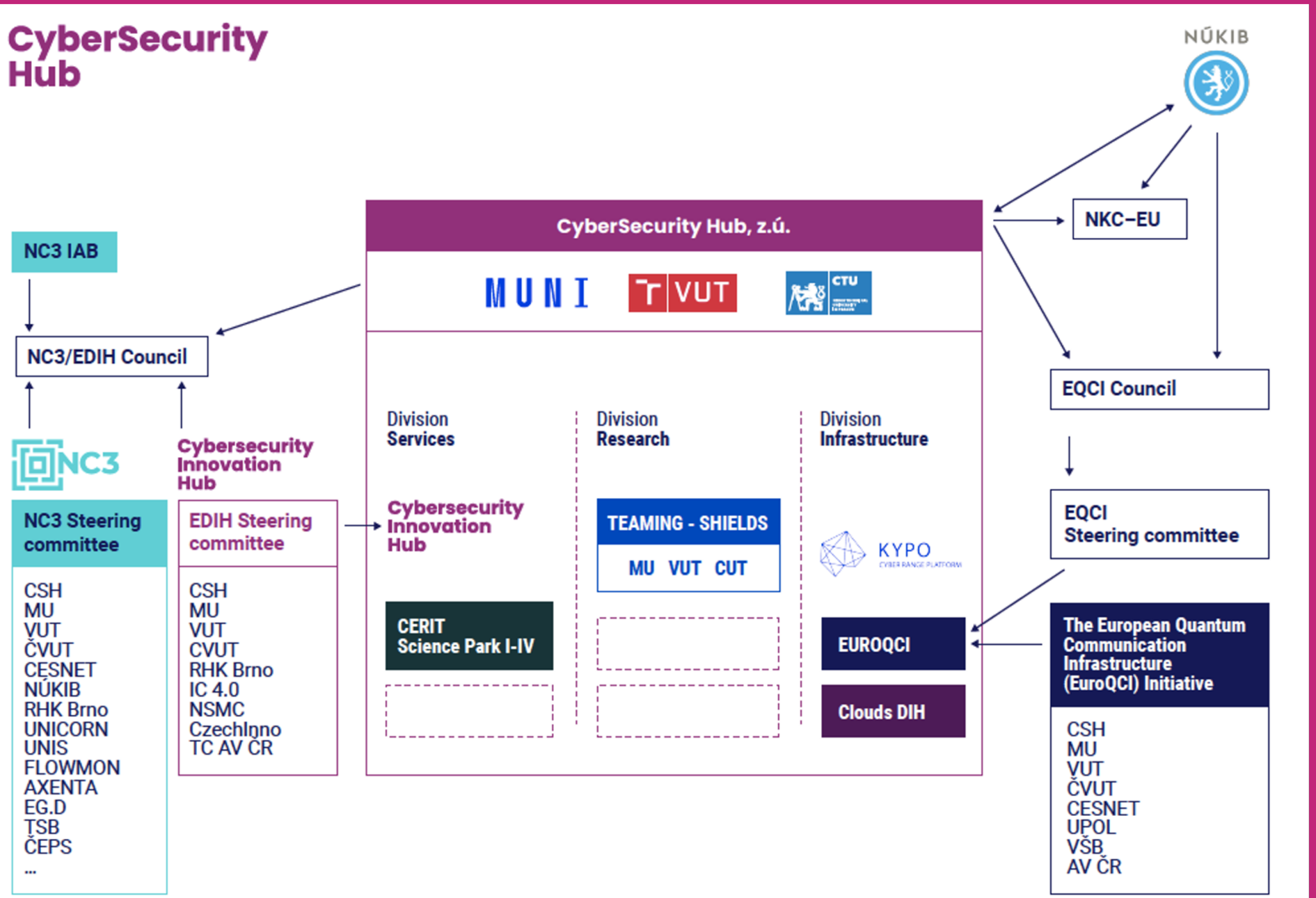
General Goals

- We increase the impact and competitiveness of Czech research and education.
- We deepen the level of our cooperation with the state, businesses and multinational organizations.
- We strengthen the resilience of the digital society and its services at all levels.

Specific Goals

- Forster international presence and increase absorption capacity of Czech cybersecurity sector
- Coordinate involvement in leading activities in Europe
  - **National Contact Center** for EU Center of Excellence in CS (Bucharest)
  - **EuroQCI** – National Point
  - **SHIELDS** – HORIZON EUROPE – Widera – Teaming

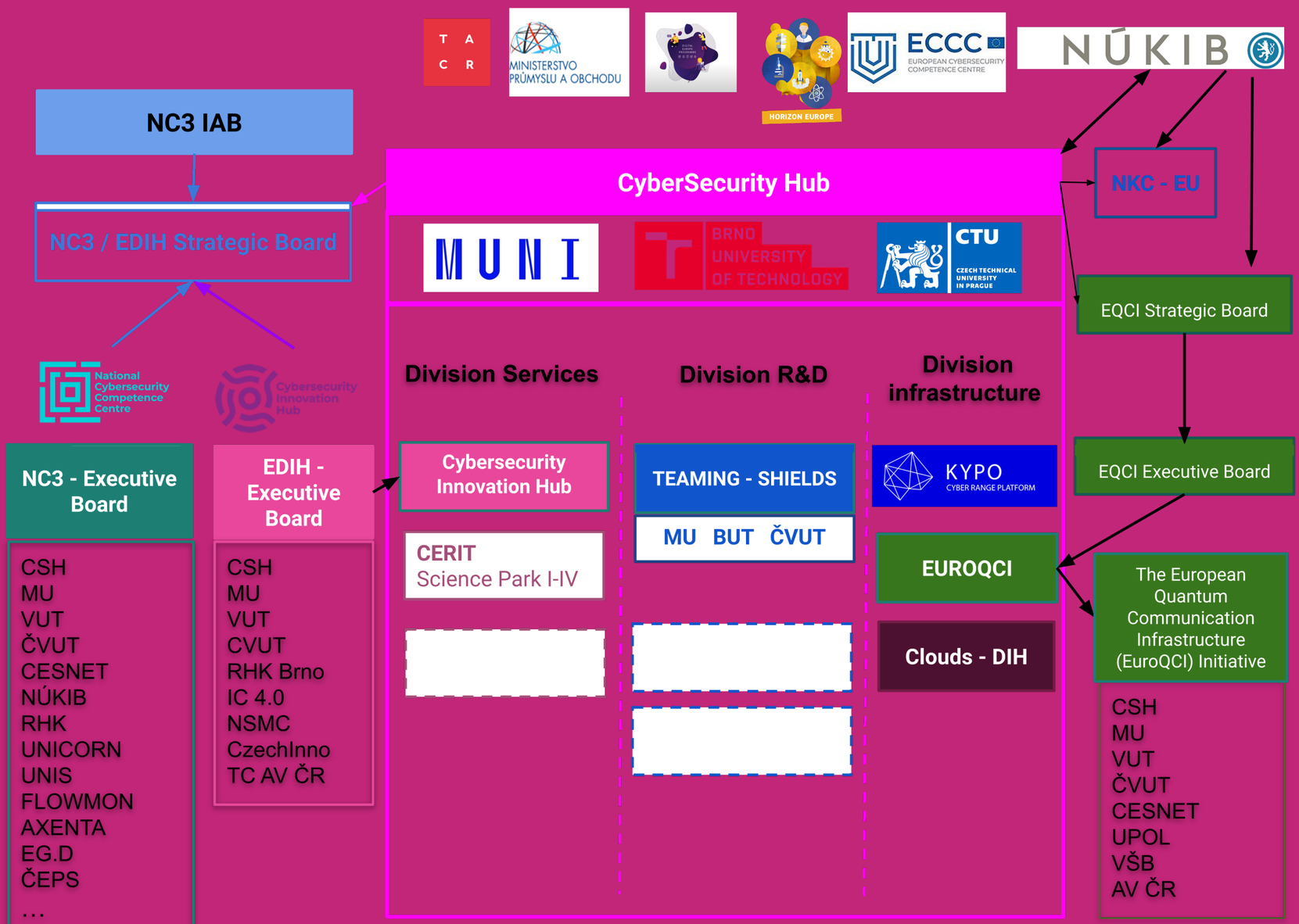
CSH – Big Picture



CYBERSECURITY INNOVATION HUB

- DIGITAL EUROPE – European Digital Innovation Hubs
- Final proposal Feb 2022. Start: 2023
- Services for SMEs and public administration
- Elaborated in close collaboration of
  - CSH – coordinator
  - CzechInno – co-leading partner
  - 3 Czech Universities
  - Partners: Chamber of Commerce, IC4.0 & Network Monitoring Clusters, Tech Center of Academy of Sciences

CYBERSECURITY INNOVATION HUB



NATIONAL COMPETENCE CENTER FOR CYBERSECURITY

- TECHNOLOGY AGENCY OF CZECHIA
- 3+3 years, cascade financing = sub-projects
- Final proposal Mar 2022. Start: 2023
- Innovation for Competition
- Value co-creation industry-academia, commercialization
  - CSH – coordinator, 3 Czech Universities
  - Partners: Unicorn, Axenta, TSB, IC4.0, NSM Cluster, CAMEA

COLLABORATION WITH CRITICAL INFRASTRUCTURE OPERATORS

- Projects of NC3, Ministry of Interior - Security Research, Technology Agency, contractual research…

- Partners: CSH, Brno University of Technology, Czech TU, Uni Pilsen
- Industry: ČEPS (Czech TSO), ČEZd (Czech DSO), ZPA Smart Energy, Mycroft Mind

R&D CHALLENGES

- Critical infrastructures – **Energy sector -** Challenges
  - Cybersecurity
  - New regulations – EU Network Codex for CS
  - Shared CS services – eSOC
  - New challenges brought by Quantum Computing, Quantum Secure Communication, Post-quantum Security
  - Standardization
  - Certification & Compliance

ENERGY SECTOR – Cybersecurity

- Energy transmission & distribution
- High risks, high or critical impact – blackout, physical damage
- Complex IT & OT & telco infrastructures
- Complex system & network architecture
- Partially separated physical infrastructure
- Physical protection
- External suppliers

ENERGY – Attack Vectors

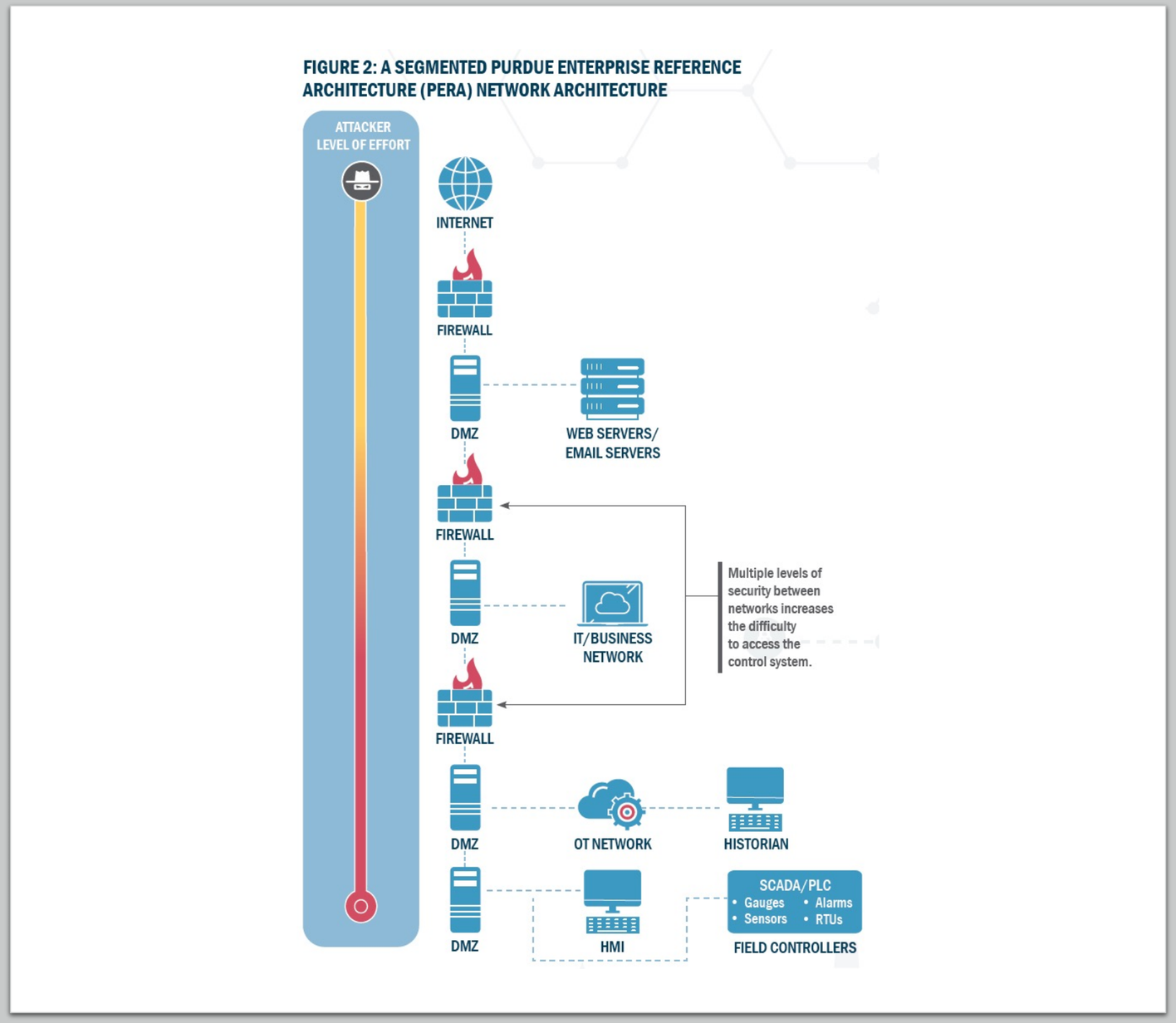
- Phishing
- Exploitation of vulnerabilities
- Use of stolen credentials
- Brute-force
- RDP
- External media

ENERGY – Security & Defense

- Resilience plan
- Training
- Hardening
- OT mapping in operation
- Risk assessment
- Monitoring 24/7

Security Principles

- ZERO TRUST
- PERA – layered architecture
- Digital Twins
- AI methods for behavior analysis



ENERGY – Attack Vectors

- Phishing
- Exploitation of vulnerabilities
- Use of stolen credentials
- Brute-force
- RDP
- External media

ENERGY SECTOR – Cybersecurity

- Serious attacks since 2015 – 1st Ukraine case
- Nation-sponsored attackers
- Sophisticated logistics
- Long time from reconnaissance
- Different (multiple) attack vectors
- Enlarged perimeter due to penetration of IoT
- Complex coverage – from OT over IT to voice communication

STRATEGIC PROJECTS

- HORIZON EUROPE – Widera – **SHIELDS** (from Q2-3 2023)
- **NC3** II (from Q1 2023)
- **Cybersecurity Innovation Hub** (from Q1 2023)
- **National Recovery Programme** (from Q3 2022)

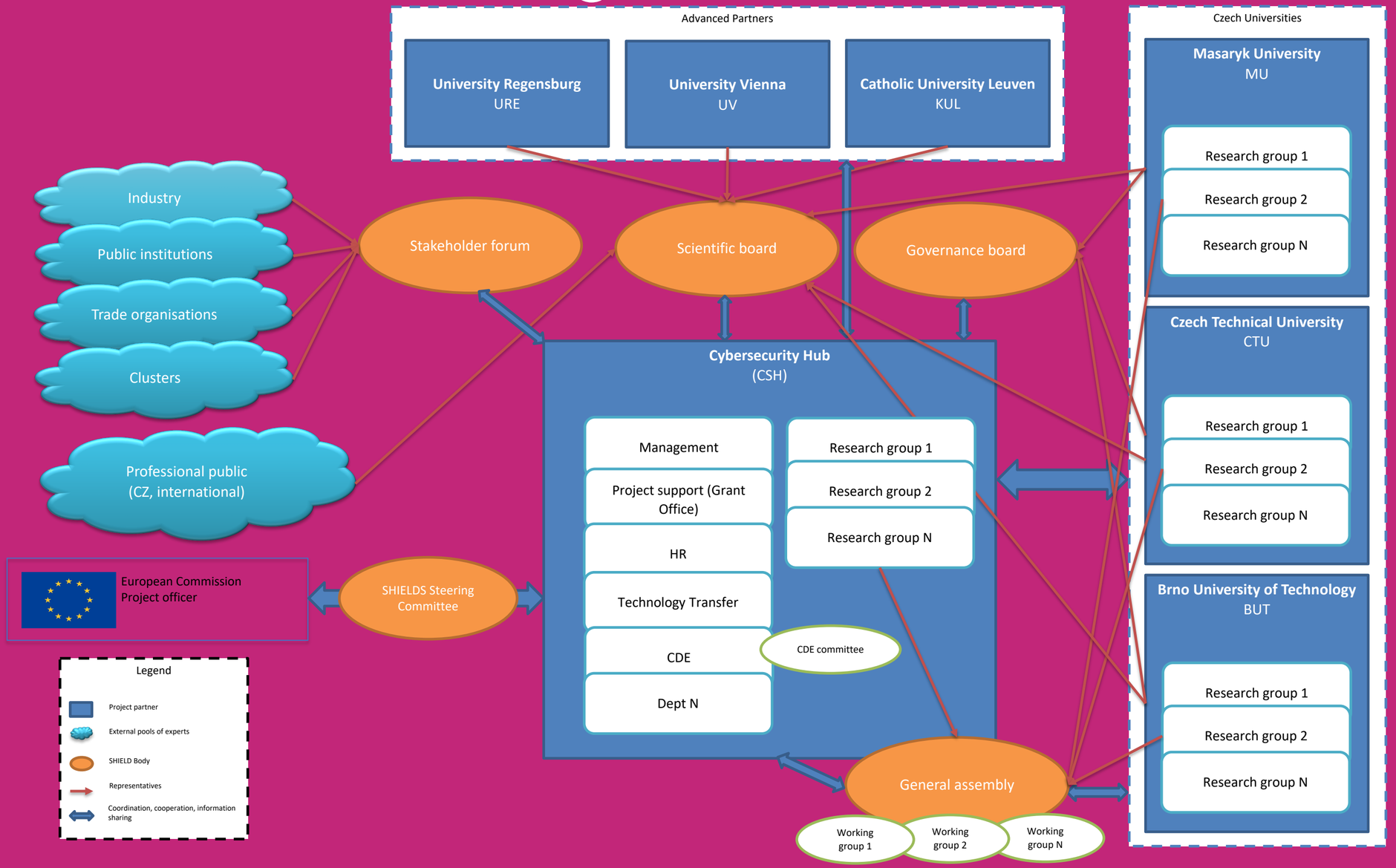
S H I E L D S

- HORIZON EUROPE – Widera – Teaming proposal in 2nd round
- Final proposal Sept 2022, Start: mid 2023
- Elaborated in close collaboration of
  - CSH – coordinator
  - 3 Czech Universities
  - 3 Partners: Uni Vienna, Uni Regensburg, KU Leuven

SHIELDS – Topics & Goals

- O1 Excellence in research
  - enhanced research capacities,
  - test beds, labs, infrastructure
- O2 Excellence in research governance
- O3 Visibility & Credibility
- O4 Bring socio-economic benefits to society
  - policy making bodies and expert groups

SHIELDS- OrgChart



SHIELDS – Expertise

- Technical Uni Brno – biometrics, privacy-enhancing technologies, hardware-accelerated cryptography, quantum and post-quantum cryptography, security in industrial and smart-grid networks, design and verification of hardware architectures, network performance monitoring and network security
- **Czech Tech Uni** – National Centre of Competency for Cybernetics and Artificial Intelligence, a platform of cybernetics and artificial intelligence for Industry 4.0, Smart Cities, intelligent transport systems and cybersecurity.
- **Masaryk Uni** – critical information infrastructure protection, namely for the power grid sector, certification and compliance in cybersecurity, cybersecurity of industry 4.0 and IoT, blockchain applications, reliable architectures, and cybersecurity education and training based on open-source **KYPO Cyber Range Platform**

SHIELDS – Expertise

- KU Leuven – secure software engineering, mobile devices, identity management and privacy, and cryptography / cryptographic protocols, analytics and (adversarial) machine learning expertise, security incident analysis (especially industrial). KUL is also the leader on security intelligence.
- Uni Vienna – process compliance and security, security & privacy techniques against vulnerabilities for modern IT infrastructures, protection of users' privacy through novel obfuscation coding or developing a protection technique, which is not possible with current methods. The most recent research looks on interdisciplinary research in blockchain
- Uni Regensburg – focuses on analysis, modelling, design, and reliable and secure use of state-of-the-art information systems in different application areas such as cyber threat intelligence, novel Industry 4.0 solutions (Secure Digital Twin Performance, up to eGovernment and e-voting)

SHIELDS – KYPO facility

SHIELDS – People in CZ

Czech University of Technology – Prague

University of Technology – Brno

Masaryk University – Brno

SHIELDS – Interest on Collaboration

Interest from industry, academia, and public organizations:

- Industrial Community – Cybersecurity, Smart Infrastructures, Autonomous Mobility, Back-end systems, Privacy
- Academic institutions from DE, CZ
- Public institutions from DE, CZ

Expression of further collaboration by a

- **Letter of Interest** to:

Tomáš Pitner, Academic Director

pitner@muni.cz

Phone: +420-778884996