Annual Conference CODE 2019

Workshop: Cyber Ranges

The implementation of a Cyber Range at Bundeswehr University Munich

Volker Eiseler

Research Institute
Cyber Defence
Bundeswehr University Munich

https://www.unibw.de/code
code@unibw.de

Agenda

- Introduction and Overview

- Learning Management System and self-learning Module
- Individual Exercises
- Example of a Scenario
- The Trainer‘s perspective

- Cyber Range related R&D projects
- Future steps

FI CODE Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

IT Competence Education & Training: I.C.E.&T.

Definition(s)

„A [Cyber Range]

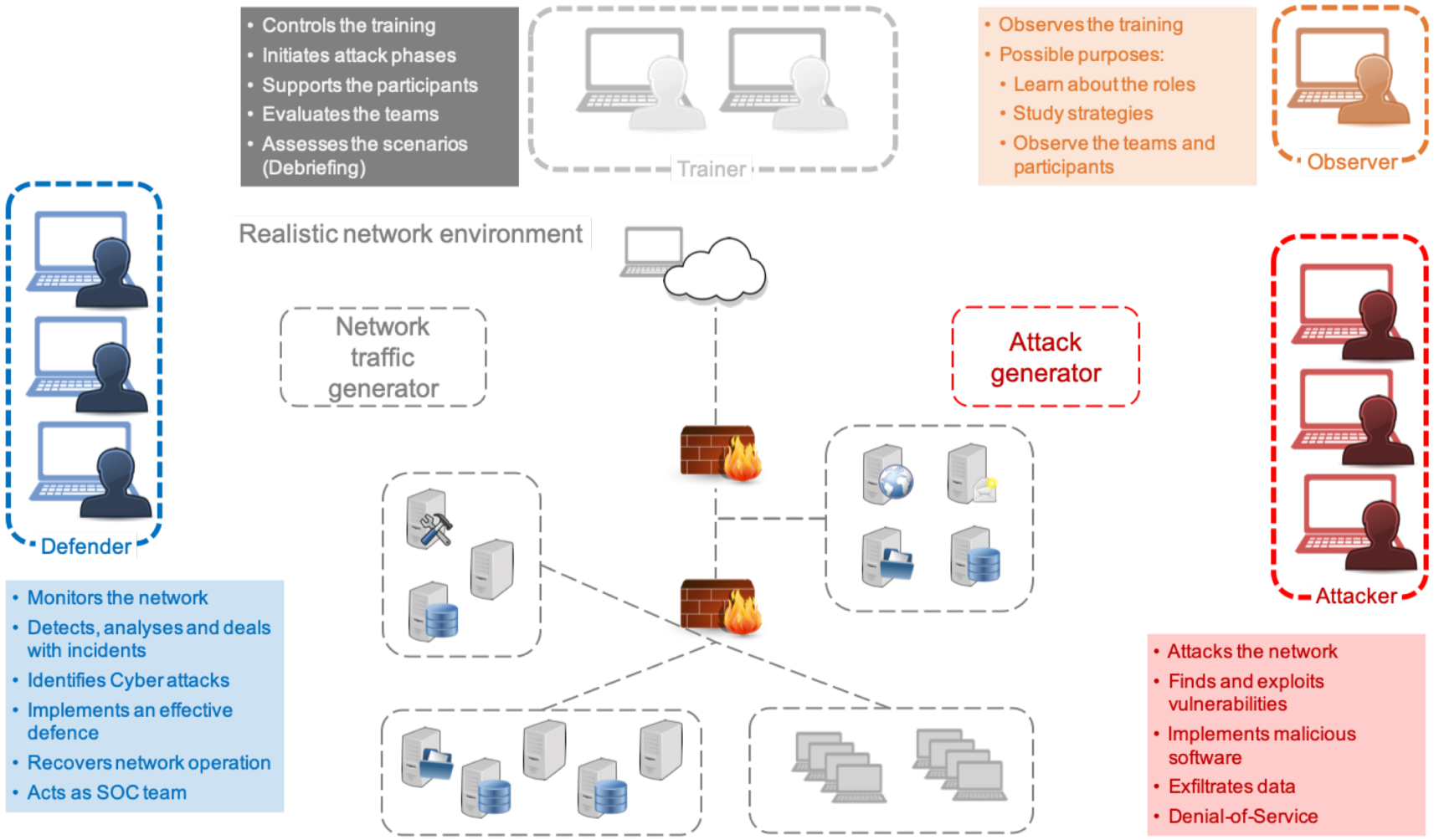
- provides an **environment to practice** CNO skills […]
- should **represent real-world** scenarios […]
- should offer isolation from other networks to **contain malicious activity** […]
- should also **support experimentation and testing** with cyber security products."

Source: J. Davis, S. Magrath: A Survey of Cyber Ranges and Testbeds. Defence Science and Technology Organisation Edinburgh (Australia) Cyber and Electronic Warfare Div (2013).

Cyber Range is a operational capability and facility in a **virtualized environment** supporting different needs:

- Safe environment for practical **cyber skills training and assessment**
  - **Integration to Master degree studies programs**
- Represents Real-World Cyber threat scenarios
- Comprehensive means for **security test** and **verification** of new Cyber security products and tools
  - Realistic simulation for improved **system testing** during development

Roles and functions

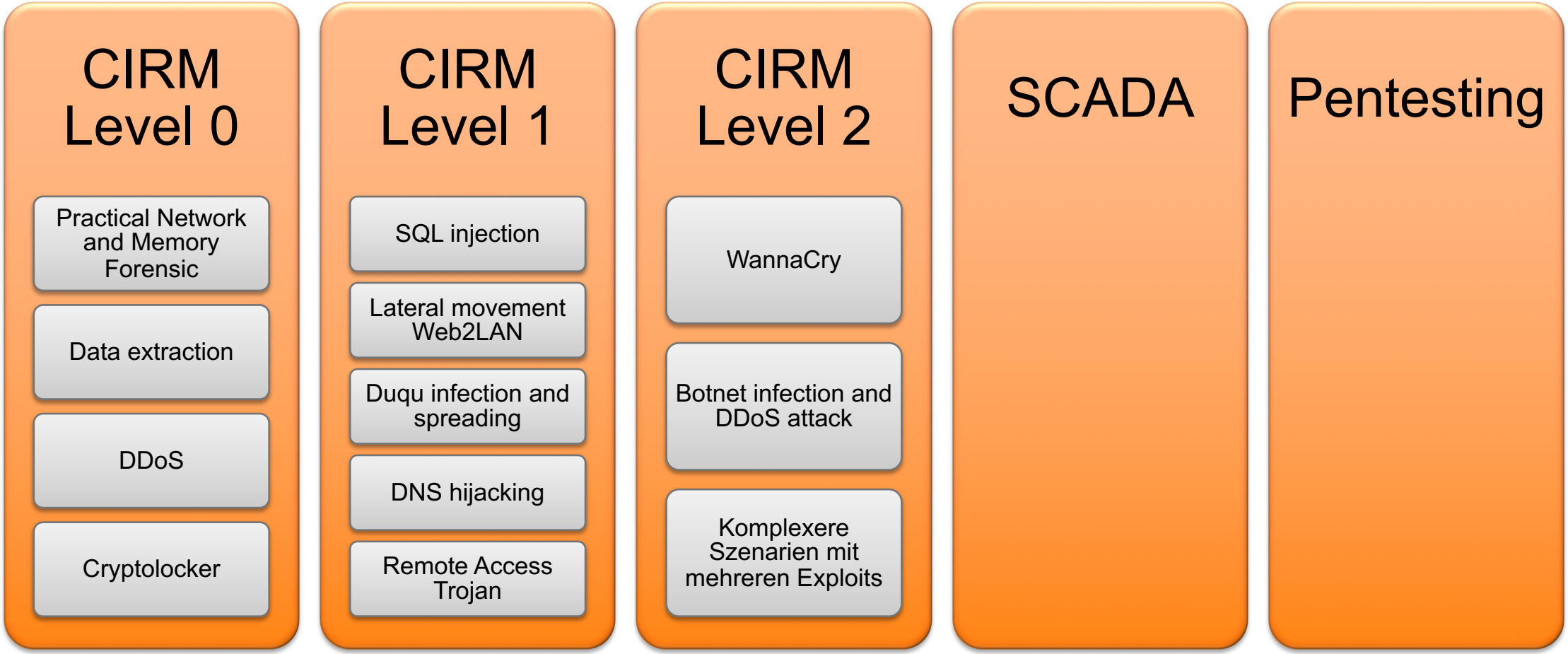


Tame Range - Overview

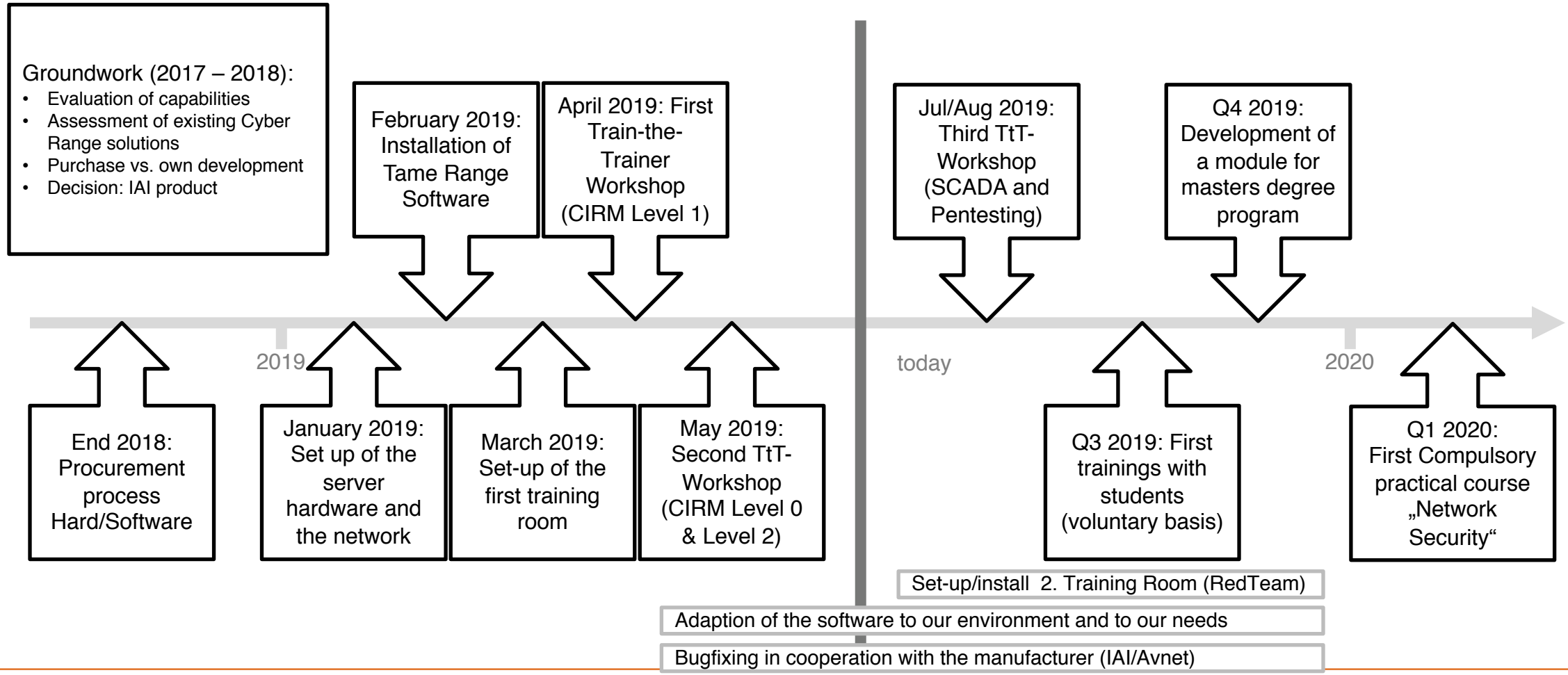
- Commercial product: IAI and Avnet (ISR)
- Comprehensive and **flexible** Cyber Range solution
- **Open,** modular platform and architecture
  - Allows to create/import and automate own content
  - Customized training environments topologies
- Pre built content:
  - 3 pre-defined virtual network infrastructures
  - Learning management system (incl. Self learning module)
  - 80 individual exercises from 9 different areas/topics

  - Pre developed complex scenarios in 3 different CIRM skill levels + SCADA + PenTesting
  - Software in order to control and assess the scenarios

Tame Range – complex scenarios



Time table for implementation



Agenda

- Introduction and Overview

- Learning Management System and self-learning Module
- Individual Exercises
- Example of a scenario
- The Trainer‘s perspective

} Demo video

- Cyber Range related R&D projects
- Future steps

Cyber Range @ FI CODE

FI CODE
Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Agenda

- Introduction and Overview

- Learning Management System and self-learning Module
- Individual Exercises
- Example of a scenario
- The Trainer‘s perspective

- Cyber Range related projects
- Future steps

Cyber Range related projects

Task: CONCORDIA's ecosystem for development and sustainability by developing virtual lab infrastructure and a federation of cyber training capabilities, services and solutions

- Interconnecting cyber range and cyber training capabilities through a portfolio platform
  - Connect Cyber Ranges with different scopes and capabilities

- Benefits:
  - Enhance Training capabilities for professionals
  - Strengthen the Cybersecurity Ecosystem across Europe
- Goals to achieve within CONCORDIA
  - Development of a portfolio platform to present a Federation of Cyber Ranges across Europe in order to provide Cyber training facilities to the consortium and to others
  - Sharing scenarios and best practice guidelines

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Cyber Range related projects

Cyber Ranges within the CONCORDIA consortium

- RI CODE / UniBw M
  - Out of the box environment/tool with own developed scenarios
  - Focus on **network security / attack-defence**
- Masaryk University:
  - Self developed virtualised environment/tool
  - Focus **network security** / red-blue-teaming
- Airbus:
  - Hybrid environment modelling **IT / OT infrastructure**
- RISE:
  - Part of RISE Cybersecurity arena and offers multiple scenarios and verticals
  - Multiple **IoT-specific** scenarios being developed
- UMIL / FORTH
  - Various aspects of cyber security training
- Loraine University (FR) / Telecom Nancy:
  - Focus on **APT attacks**

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Cyber Range related projects

Research Project (R&D) with BAAINBw and BMVg

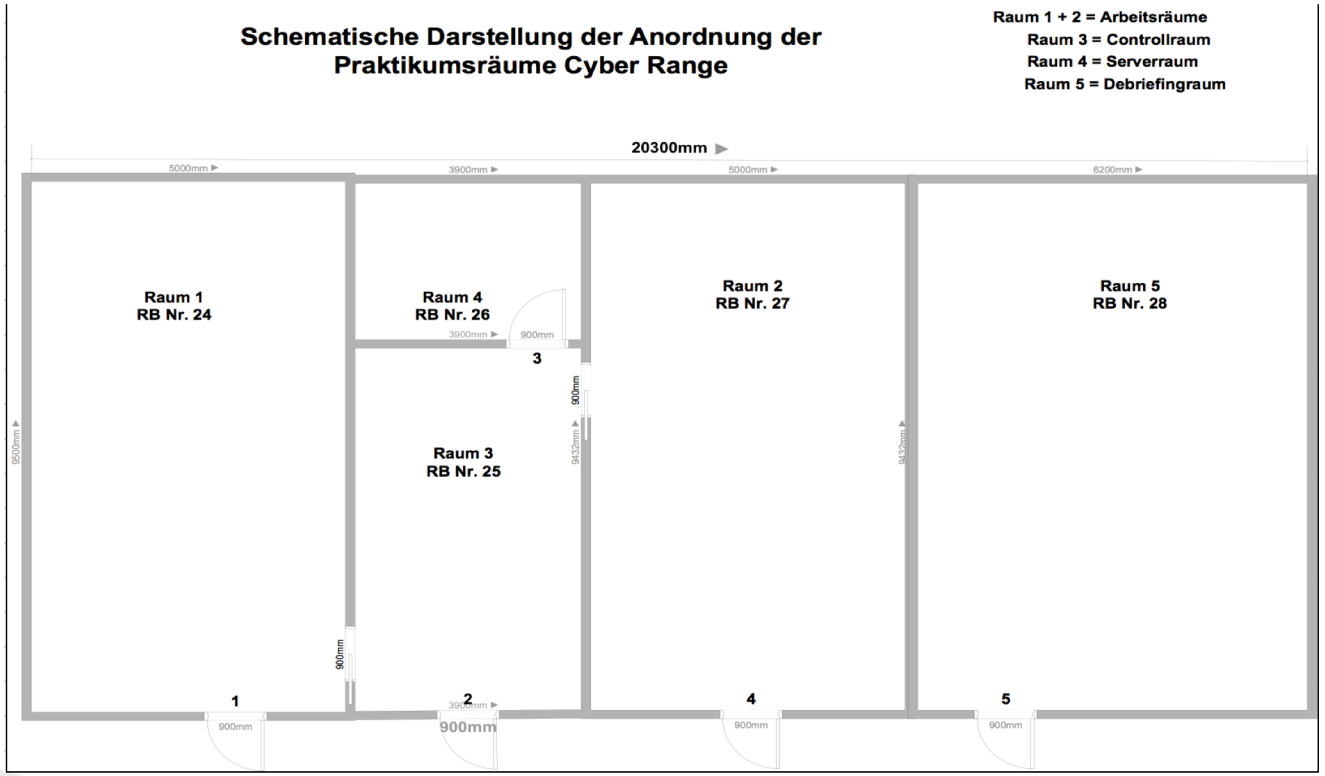
Goals

- Design and use of Cyber Ranges, regarding cyber technology development, system testing, and operations training
- Improve the exchange of tools, architectures, as well as concepts and where applicably technical equipment in the context of Cyber Range; e.g.
  - Module for automated network mapping and integration to the Cyber Range (customizing the Cyber Range)
  - Module to simulate various network architectures
  - Automated traffic generation
- Development of a Cyber Range environment for common tests and trainings as well as IT based joint exercises for cyber experts

Future steps

- Integration of the Cyber Range into the curriculum (Master study program)
- Extension of the Cyber Range capabilities
  - New equipment
  - Integration of new hardware and software
- Development of own scenarios
- Continuation of Research Projects
  - CONCORDIA
  - R&D project in cooperation with the Ministry
- Providing cyber trainings to Bundeswehr and other partners

Future steps



Summary

Existing solution provides various functionalities

First step:

- Trainings for students in the Masters degree program Cyber Security

Flexible Interfaces allow integration of

- New, own scenarios
- Different networks and architectures

FI CODE Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

https://www.unibw.de/code
code@unibw.de