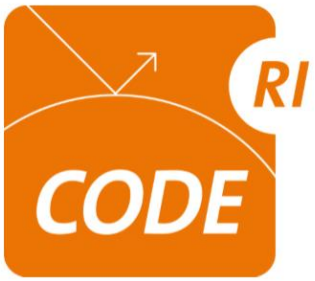

Research Institute
Cyber Defence
Bundeswehr University Munich

Summary of workshop 2 „Cyber Resilience of Critical Infrastructures"

Organizers:

Kevin Mallinger (SBA Research)

Mario Drobics (AIT – Austrian Institute of Technology)

Moderator:

Philipe Reinisch (http://www.boteillier.com/#contact)

Content:

In this workshop, resilience in the context of software systems was discussed and prepared in the respective blocks "Cyberresilience", "Complex Networks" and "Supply Chain Resilience".

The keynote was held by **Victor Galaz (Deputy Director of the Stockholm Resilience Center**) who presented the global context of resilience and discussed the slow variables of change that are, ultimately, the overall framework for short term disruptions.

Followed by an introduction **by Kevin Mallinger (SBA Research),** who spoke about the systemic compounds of complex cyber-physical systems and the patterns of resilience. Different notions of resilience have been discussed and a working definition has been established. The goal was to create the scientific basis for the upcoming presentations.

The next speaker was **Martin Latzenhofer (AIT – Austrian Institute of Technology)** who talked about the approach of AIT for organizations to cope with novel cybersecurity threat patterns. He pointed out, that not only critical infrastructure but all the players in an economic market are becoming more and more vulnerable. The overall objective is to get these systems resilient against known and even new threats raising up on the threat landscape.

Sebastian Thölert (Bundeswehr, Referent Cyber Awareness), Andreas Klein (Kdo Lw) and Gernot Schwierz (IABGmbH) discussed resilience in complex operational scenarios. They presented, that the own complex structural and operational organization is sufficiently represented technically in order

to compare it with a threat situation. The aim and purpose is to draw conclusions about the effects of attack vectors in your own organizational and operational structure from different perspectives.

Corinna Schmitt (Bundeswehr University Munich) spoke about the combination of IoT with AI. She presented, that AI can be used in different IoT applications in order to predict behavior or learn from old data in order to establish trust in an application or service. She further introduced the concept of AI and how it can be combined with IoT praradigms to strengthen trust in IoT.

Mario Drobics **(AIT – Austrian Institute of Technology)** talked about the Resilience and trustworthiness in complex IoT environments. He provided an overview on different dimensions of trust, and how these concepts can be applied in concrete use-cases like smart-cities or automated driving in order to increase resilience and acceptance of these applications.

Later, **Werner Strasser (Fragmentix)** presented secret sharing appliances for privacy, digital and resilience in the cloud.

The last presentation was held by **Stefan Jakoubi (SBA Research)** who talked about the connection of supply chains and cyberresilience. The center of his talk was focused on value creation within a secure environment. Furthermore, he discussed the critical appreciation of scarcity of resources, the development to cost(!) efficient monocultures and the contradiction to necessary diversity.

Future potentials and challenges:

One of the main challenges within the cyber-resilience community can be seen in the broad topic of communication. As most technologies to create resilient systems are already at hand, shortcomings can be found in the distribution and coordinated communication of know-how, data and information.

General challenges in communication can be seen in:

- the ability to share best practice examples with relevant stakeholders
- the creation of safer and faster ways for the exchange of **relevant** data
- the enhancement of the reliability of communication
  - battling the fake-news problem
  - identifying reliable sources
  - sorting out invalid information
  - enhancing the transparency of facts
- to communicate the most urging problems/threats of society to politics, companies, institutions and society in general
  - to gather the right technologies
  - involve the right stakeholders
  - increase cooperation to foster fast and effective responses to threats

Further examples of challenges can be found in the modelling of complex systems and emergent behavior, socio-technological imaginaries of complex systems, management biases for handling complex environments, or the unsecure development of IoT.