Assessing the Security and Resilience of Mobile Broadband Networks for PPDR

P. Smith, S. Schauer, A. Gouglidis, D. Hutchison,
P. Van Mieghem, R. Kooij, G. Ventre
paul.smith@ait.ac.at

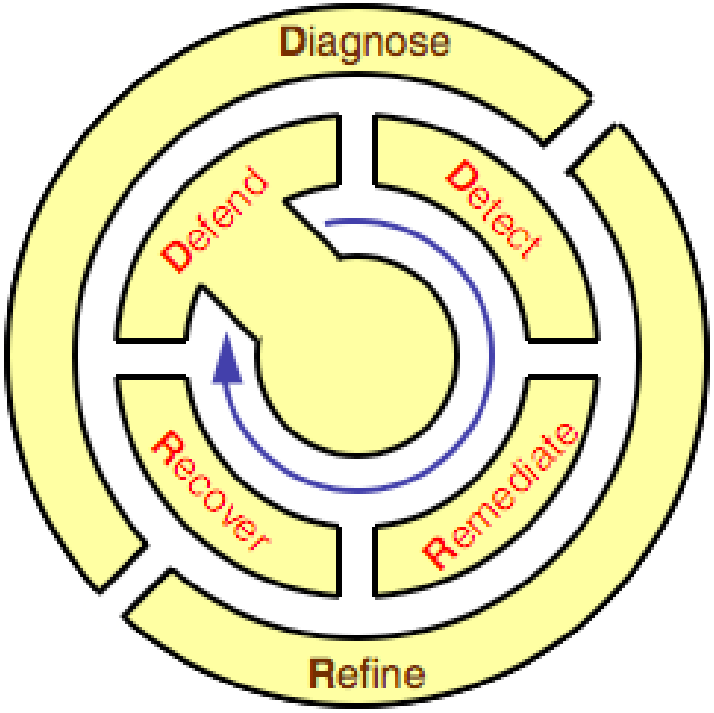
Senior Scientist
AIT Austrian Institute of Technology
Digital Safety & Security Department

"… the ability of a network to defend against and maintain an acceptable level of service in the presence of challenges"

A Strategy for Network Resilience

D^2R^2 + DR consists of 2 loops

- Real-time control (internal) loop
- Background (external) loop

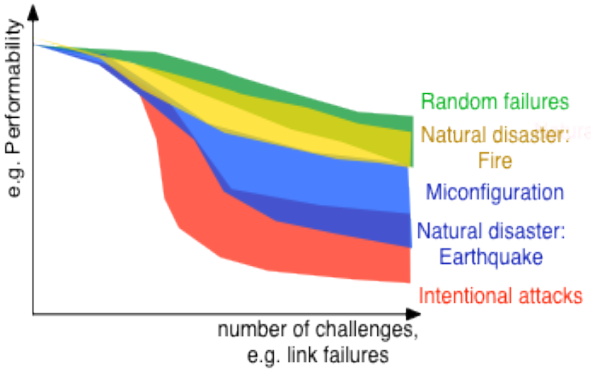


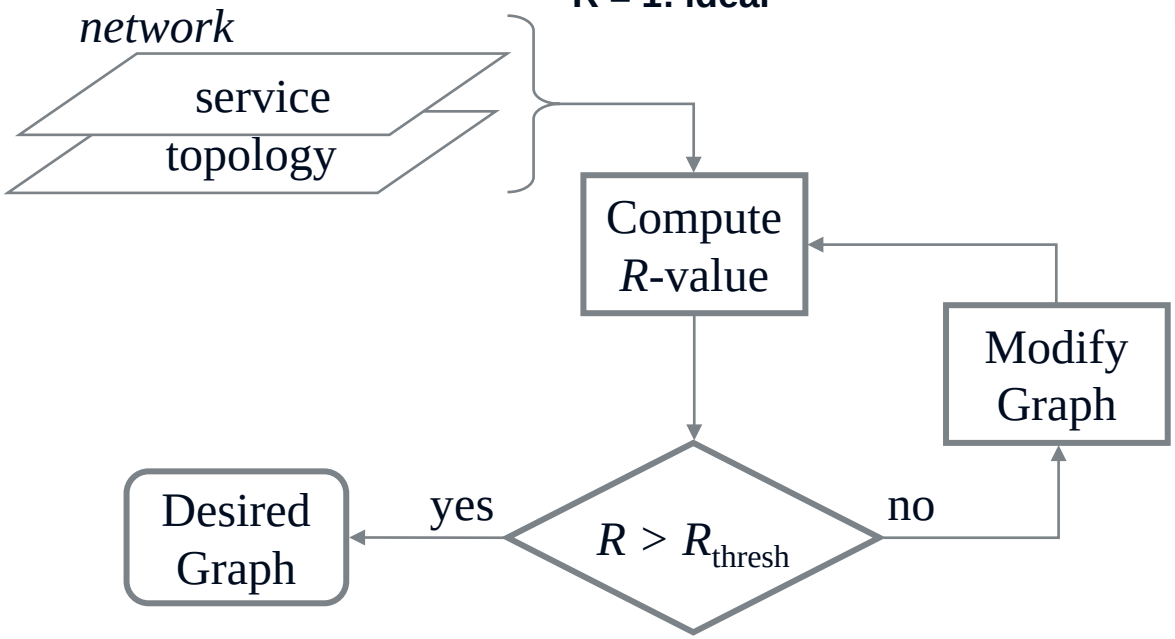
Partially validated in:

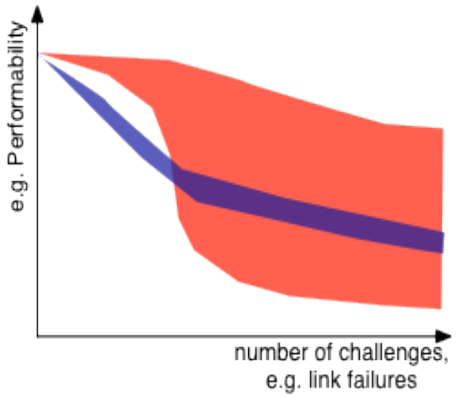
James PG Sterbenz, et al. "Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines." Computer Networks 54.8 (2010): 1245-1265.

Measuring the Resilience of Networks – the R Value

R-value: network robustness metric
R = 0: no robustness
R = 1: ideal





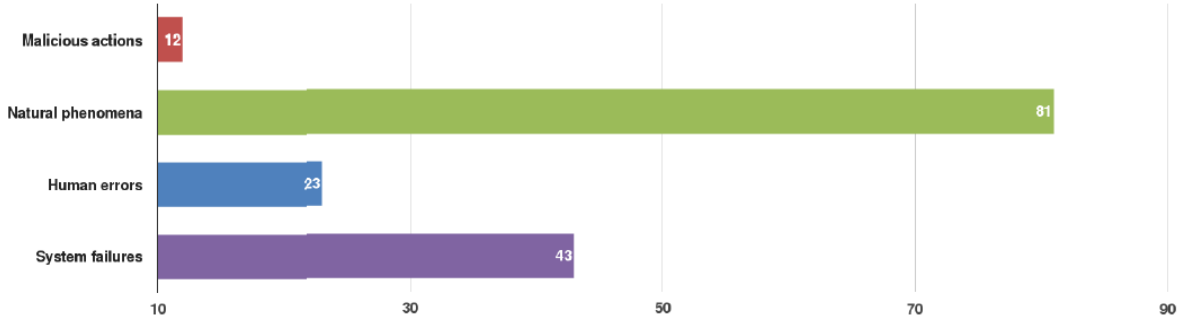


P. Van Mieghem, C. Doerr, H. Wang, J. Martin Hernandez, D. Hutchison, M. Karaliopoulos and R. E. Kooij, 2010, "A Framework for Computing Topological Network Robustness", Delft University of Technology, report20101218.

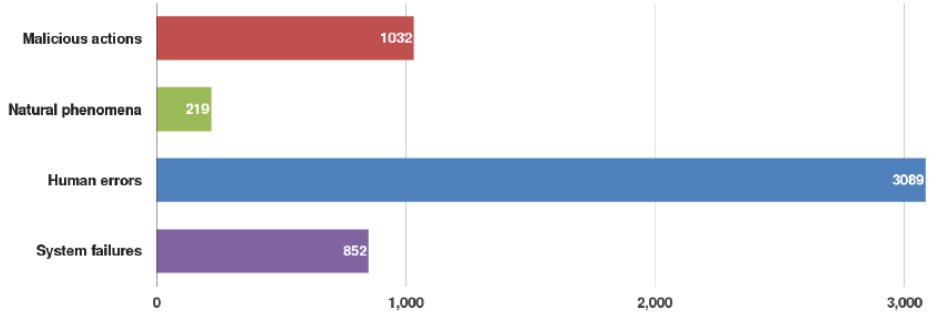
The Nature of Resilience Challenges: Incident Classes

- **Natural phenomena** – severe weather, earthquakes, floods, pandemic diseases, wildfires, wildlife, and so on.
- **Human errors** – errors committed by employees of the provider or outside the provider, during the operation of equipment or facilities, the use of tools, the execution of procedures, etc
- **Malicious attacks** – a deliberate act by someone or some organisation, e.g. a Denial of Service attack disrupting the service, or a cable theft.
- **System failures** – technical failures of a system, for example caused by hardware failures, software bugs or flaws in manuals, procedures or policies.
- **Third party failures** – a failure or incident at a third party. The category is used in conjunctions with one of the other four root cause categories.

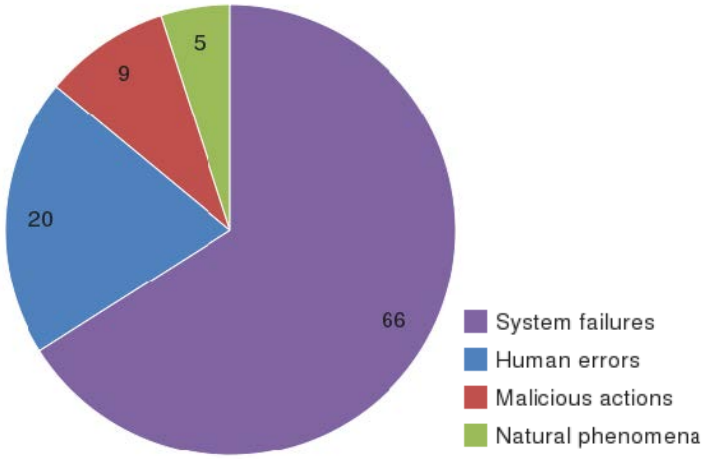
The Nature of Resilience Challenges



Average duration of incidents per root cause category (hours).

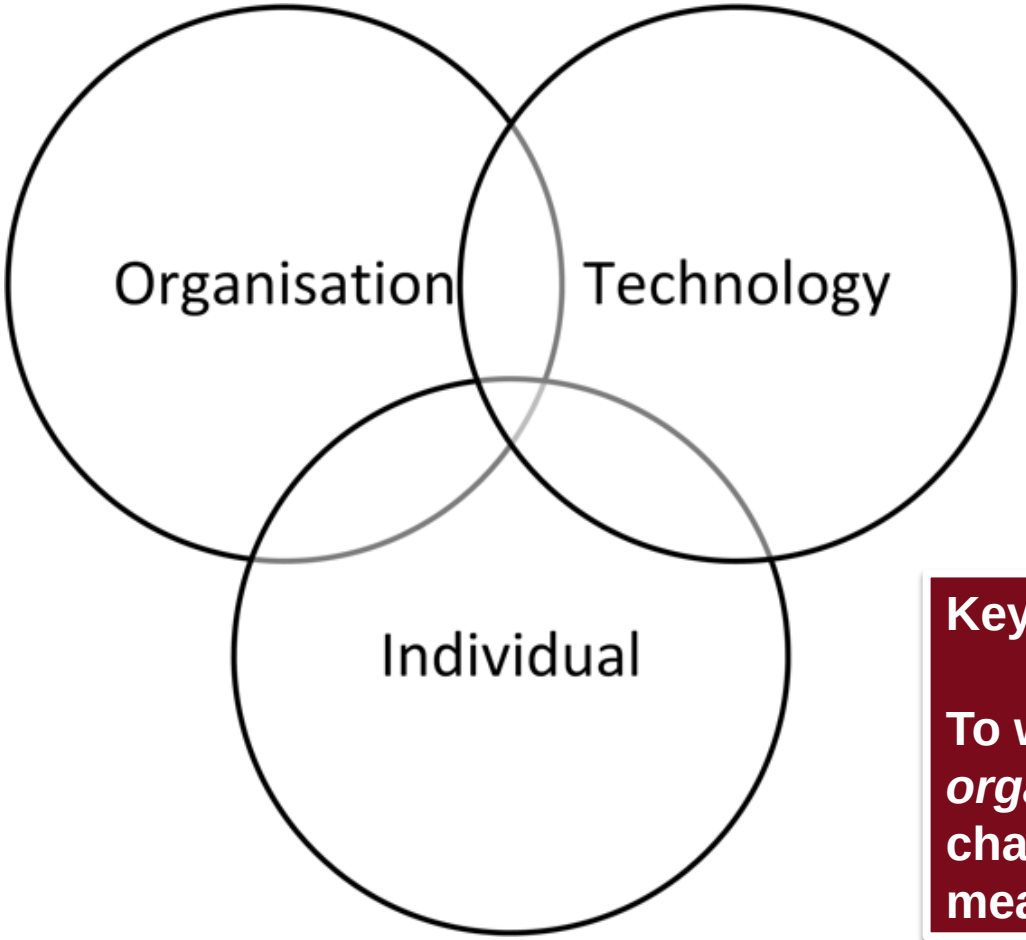


Average number of user connections affected per incident per root cause (1000s)



% Incidents per root cause category

Resilience Challenges Are Therefore …



Key question:

To what extent are *organisation* and *individual* challenges computable to get a measure or resilience?

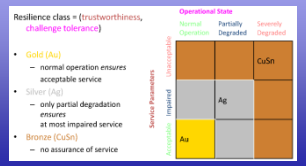
An Approach to Measuring Resilience

AUSTRIAN INSTITUTE OF TECHNOLOGY

Analysis

Measure, Derive

Resilience Classes



An abstraction to support the specification of desired resilience indicator levels

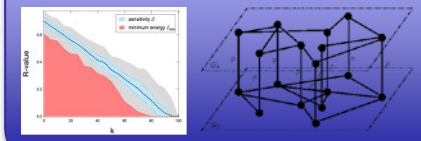
Resilience indicator R = [0,1], relate to Resilience Classes

Resilience Indicator R

Critical infrastructure specification, including technical (ICT), target infrastructure, organisational aspects, ...

Critical infrastructures in which ICT plays an important central role

R-value Evaluation



Metric Envelopes, Coupled network analysis, measuring cascading effects, ...

Evaluate monetary cost, social well-being, safety and reputation risks

Consider Resilience Indicator R in terms of important socio-economic risk factors

Threat Specification: natural, human, (un)intended, ...

A broad variety of threats considered

Conclusion

- Ensuring the **resilience** of mobile networks for PPDR is as important as **security**
  - For various reasons, malicious actors will succeed in compromising these systems, and networks must remain operational
- It is important to take an approach that considers **resilience by design**, e.g., based on the D^2R^2+DR strategy
  - To determine how effective a design is, we need suitable **metrics** and approaches to **measuring resilience**
- Resilience challenges are **technical**, **organisational** and **individual** in nature
  - A key research challenge is determining methods for measuring these aspects in a unified manner

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

AIT Austrian Institute of Technology

your ingenious partner

Dr Paul Smith
Senior Scientist
Digital Safety & Security Department

paul.smith@ait.ac.at | +43 664 883 90031 | www.ait.ac.at/it-security