Threat Awareness for Critical Infrastructures

Antonios Gouglidis – Lancaster University

Novel Approaches to Risk and Security Management for Utility Providers and Critical Infrastructures

Vienna 02.11.2015

Outline

- Motivation & objectives
- Approach on threat identification
- Overall approach for threat awareness
- Case study

Motivation & Objectives

- Importance of protecting CI
- Threats on the rise
- Serious cyber attack believed likely

- Investigate threats
- Provide foundations
  - Novel protections
  - Prevention mechanisms

OTI Viewpoints

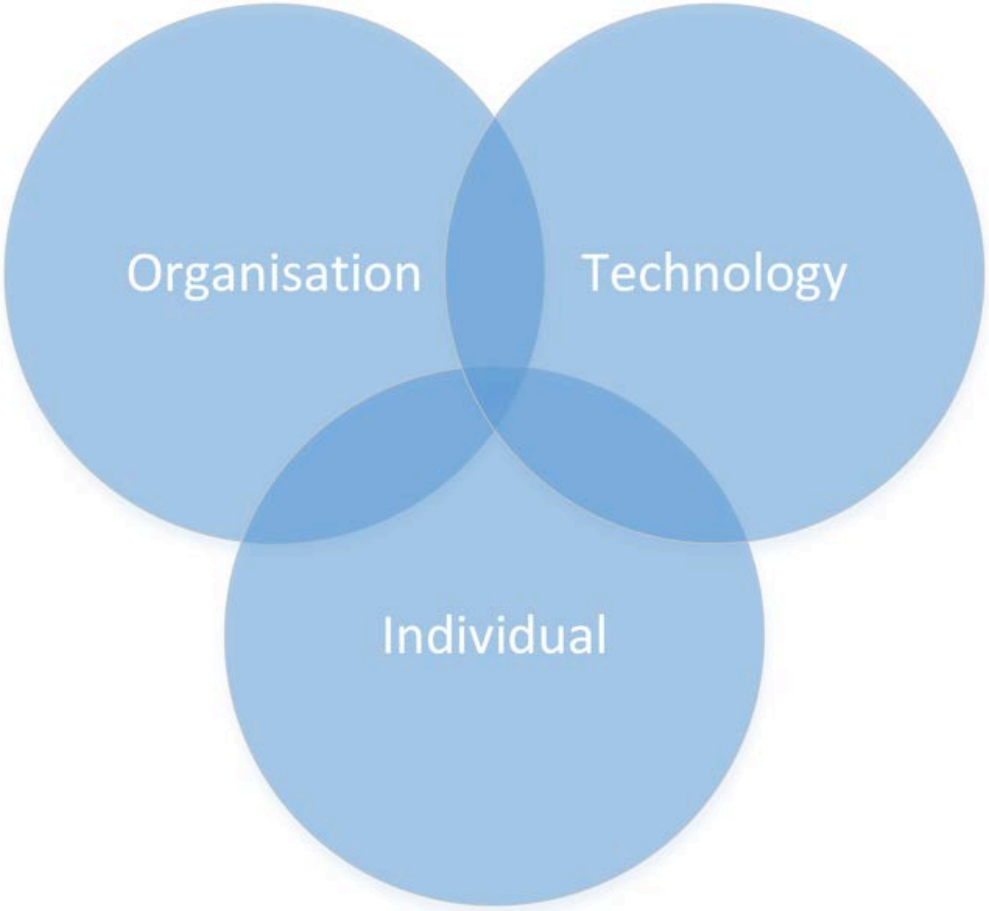


Fig. 1: Viewpoints for utility networks

Threats stemming from...

- Sources of examined threats: ENISA, NIST, ISO/IEC.

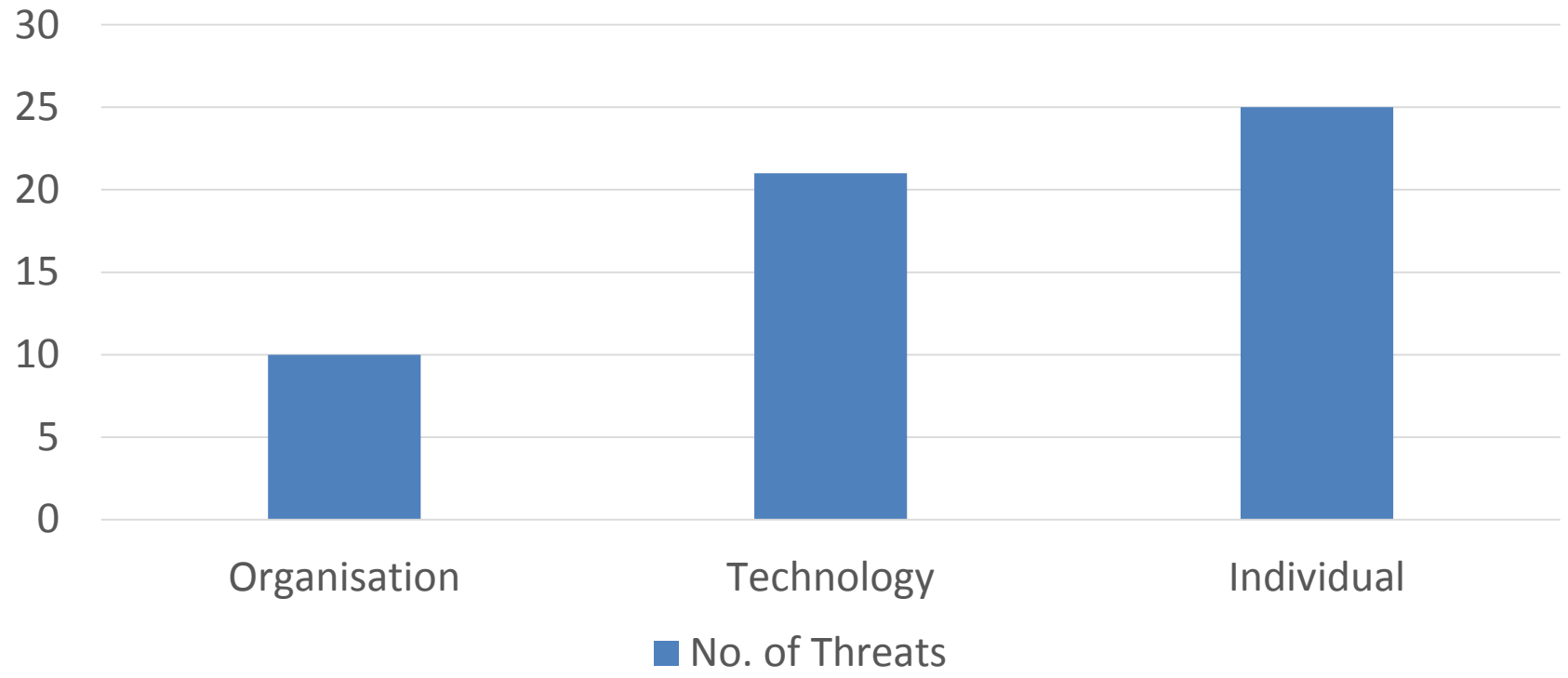
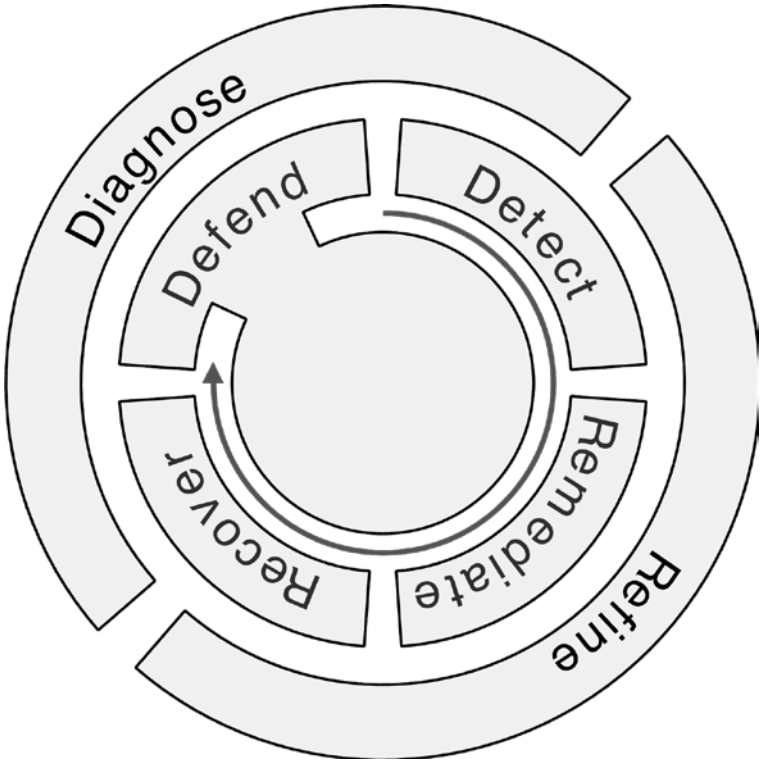


Table. 1: OTI based classification of threats

Towards Security & Safety in CI

Fig. 2: “Onion” approach

Ways of achieving resilience…



- D^2R^2+DR has 2 loops
  - Real-time control (internal) loop
  - Background (external) loop

Fig. 3: Resilience strategy

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

Set processes for threat awareness

- Situational awareness (SA)
  - *"… within a volume of time and space, the perception of an entreprise's security posture and its threat enviroment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future." **

Fig. 4: The three phases of threat awareness

* Committee on National Security Systems CNSS Instruction No. 4009

Overall architecture

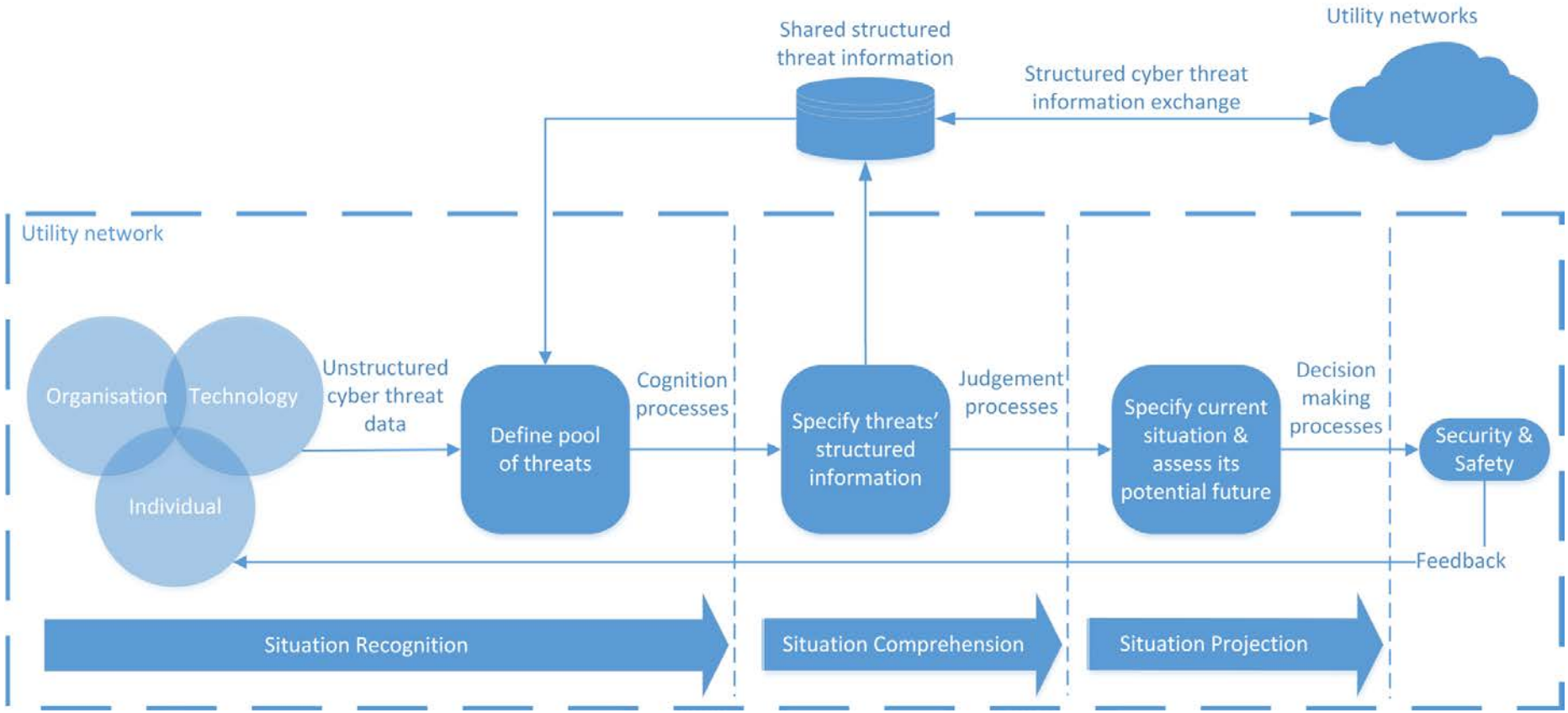


Fig. 5: Threat awareness

Case study: impact of social eng.

Situation Recognition	• System and e-mail access review • Interviews
Situation Comprehension	• Technical vulnerability assessment • Compromise graph preparation
Situation Projection	• Examination of compromise graph • Security controls, training, …

Findings…

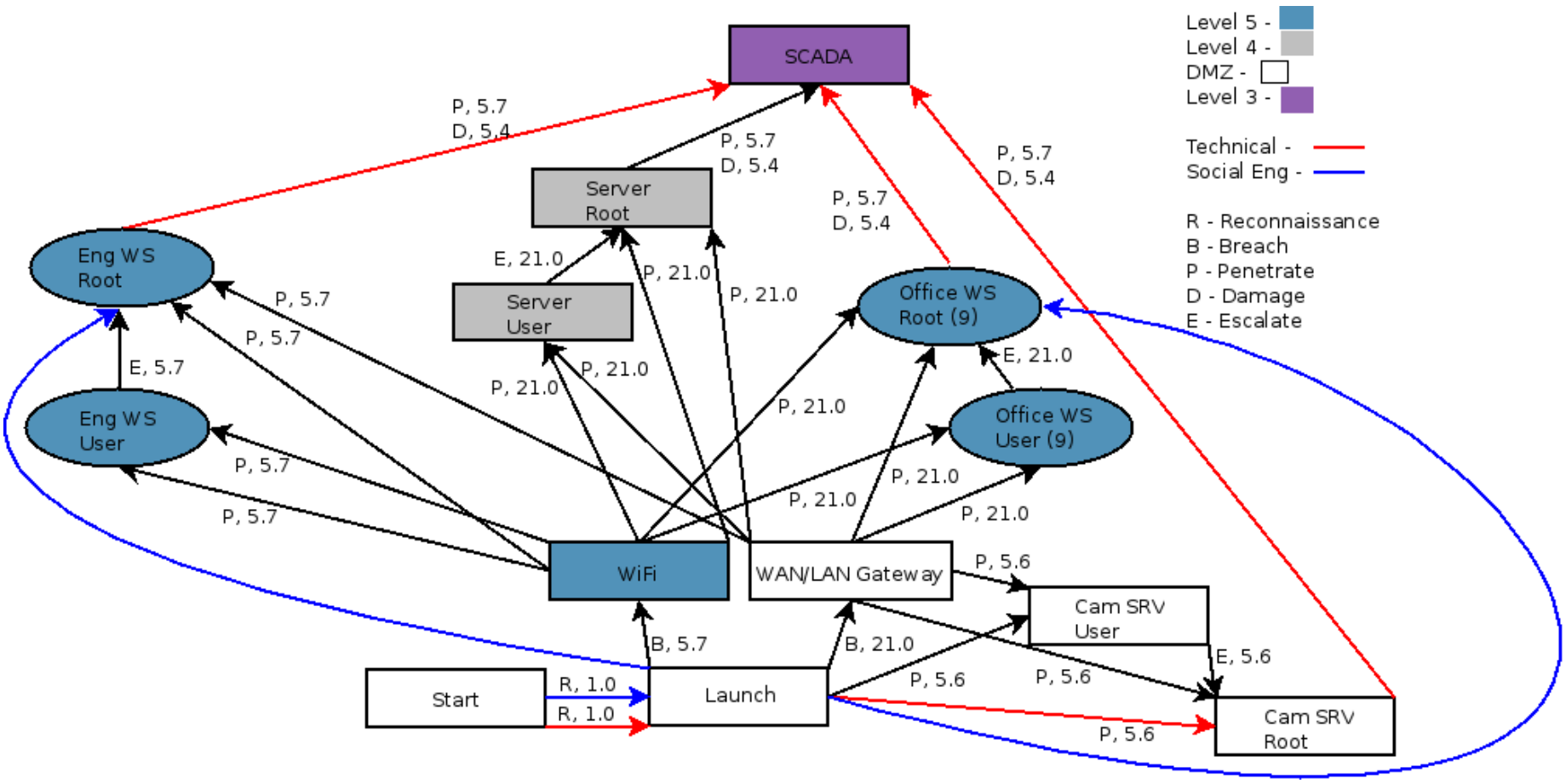


Fig. 6: Compromise graph

EUROPEAN COMMISSION

Questions?

HyRiM

Contact

- If you would like further information contact the HyRiM project members via the
- Web page: www.hyrim.net

- HyRiM is also on:
  - LinkedIn
  - ResearchGate
  - XING

HyRiM Partners

This project is supported by the European Commission
through the FP7-SEC-2013-1
Grant Agreement Number: 608090