

---

forward»

**forward»**

Managing Emerging Threats  
in ICT Infrastructures

---

# Project Motivation

---

**forward**»

**forward**» is a coordination action to bring together

- academics,
- industry, and
- policymakers ...

who are interested in emerging threats to ICT infrastructures

- ICT is a complex field
  - involves many domains and changes rapidly
  - affects systems outside the network

Need for coordinated research activity and multi-domain cooperation

# Project Objectives

---

forward»

- Establish working groups
  - effort to perform deep analysis of ICT threats
- Set up community platform
  - continuous review of threat landscape and dissemination of results
- Organize workshops
  - bring together players for face-to-face exchange
  - foster community building
- Compile threat scenarios
  - summarize working group findings
  - outline future research roadmaps (white book)

# First Workshop

---

forward»

- End of project phase I
  - establish online platform
  - hold workshop
- Identify relevant partners
  - make project known and invite potential working group participants
  - threshold for success was 30 attendees
  - significantly exceeded
- Define working group topics
  - this is why we are here ...

# Workshop Format

---

forward»

- Plenary sessions
  - impulse talks to rapidly get views from different angles
  - Threats on the Internet - Seminar
- Brainstorming sessions
  - labeled with preliminary working group titles
  - examine suitability and depth of topic
    - identify emerging and future threats
    - identify current research efforts and required, additional resources
    - reflect on-going work and best practices
  - there will be moderators and note-takers present
  - procedure to select a session

# Preliminary Working Groups

forward»

- Large-scale systems (VU)
  - large software system made of components, large number of inter-connected systems (RFID, sensor nets), ...
- Networks and monitoring (FORTH)
  - Internet backbone, routing, social networks, privacy, ...
- Malware (TU Vienna)
  - analysis and detection, evasion, possible impact (physical harm), ...
- Fraud (Institute Eurecom)
  - underground economy, social engineering attacks, financial system, ...
- Critical infrastructure protection (Chalmers)
  - how attacks against the ICT network can affect the “real-world”