Why care?

- Collateral damage / DDoS attacks
Regulatory

- Mandatory firmware update
- End of life
  - Inform customers (e.g., sticker on the device)
- Do we need a remotely executed IoT TUeV?
- Scope of the guarantee for users about their devices (what gets updated)?
  - Example: Car safety - recall actions
Operational

• Kill switch: under what conditions should a device be disabled?
• Update of already deployed devices (not enough flash, RAM, etc.)
• Segmentation of networks to sandbox devices.
• How to identify malicious devices?
  – Example: Windows Defender (repository of security bugs and how to check for them)
Proxy & Edge Computing

- Does it increase the attack surface?
- How to authorize to act on behalf of cloud-based service?
- How can services be executed securely? (role of hardware support)
- How to know to trust other communication devices? (machine learning, attestation, ..)
The User

• Incentive problems: devices work but cause problem on the Internet
• How to inform users about security problems of their devices?
• What should be the role of the operator to quarantine devices? Should the operator inform the user?
• Does he pay for security? Do we need a new business model for IoT devices based on subscription?