SaTC: CORE: Small: Towards Robust Moving Target Defense: A Game Theoretic and Learning Approach

Challenge:

- Interplay between system dynamics, security, and incentives
- Intelligent, stealthy, and persistent attacks
- Necessity of coordinating multiple defenders

Solution:

- Markovian Stackelberg Games for efficient spatial and temporal decisions in large-scale MTD
- Thwarting unknown attacks via online learning from noisy and adversarial data
- Strategic information sharing and hiding in multi-player MTD
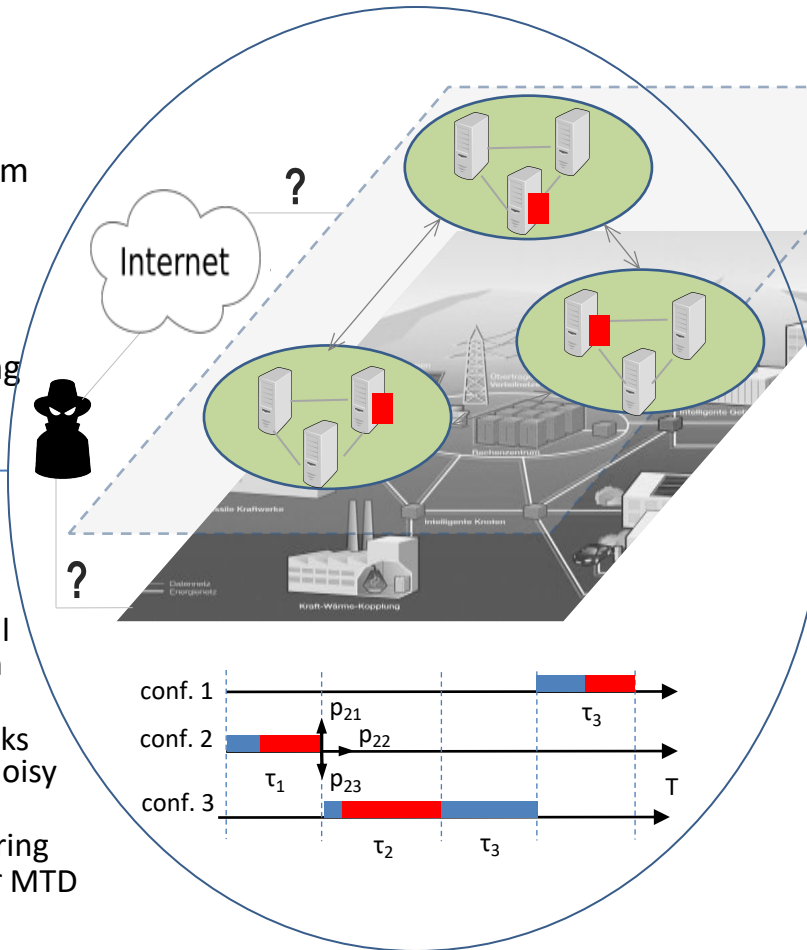
Scientific Impact:

- A rigorous approach to the design and analysis of active defense against stealthy attacks
- Deep insights on information asymmetry and the use of continuous learning in cyber attack and defense

Broader Impact:

- A cross-disciplinary approach to cybersecurity
- New game theoretic and learning methods for decision making beyond cybersecurity
- 1 graduate student and 1 undergraduate coordinate major student involved (1 postdoc and 2 undergraduates joining)