SARnet

Dr. Paola Grosso
Associate professor

Systems and Networking Lab
Multi-scale Networked Systems

Universiteit van Amsterdam

System and Network Engineering

Attacks on networks

Attack on routing element, exploiting protocols design ‘flaws’

Attacks on end points servers

Attacks on physical infrastructures

Attacks on networks

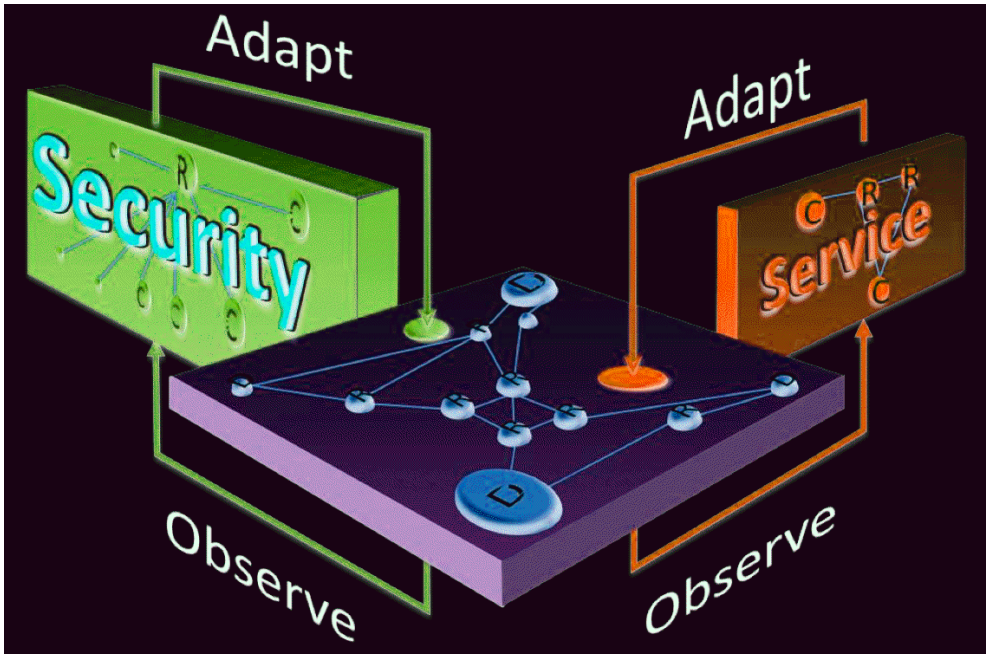
- Attack on routing element, exploiting protocols design ‘flaws’
- Attacks on end points servers
- Attacks on physical infrastructures

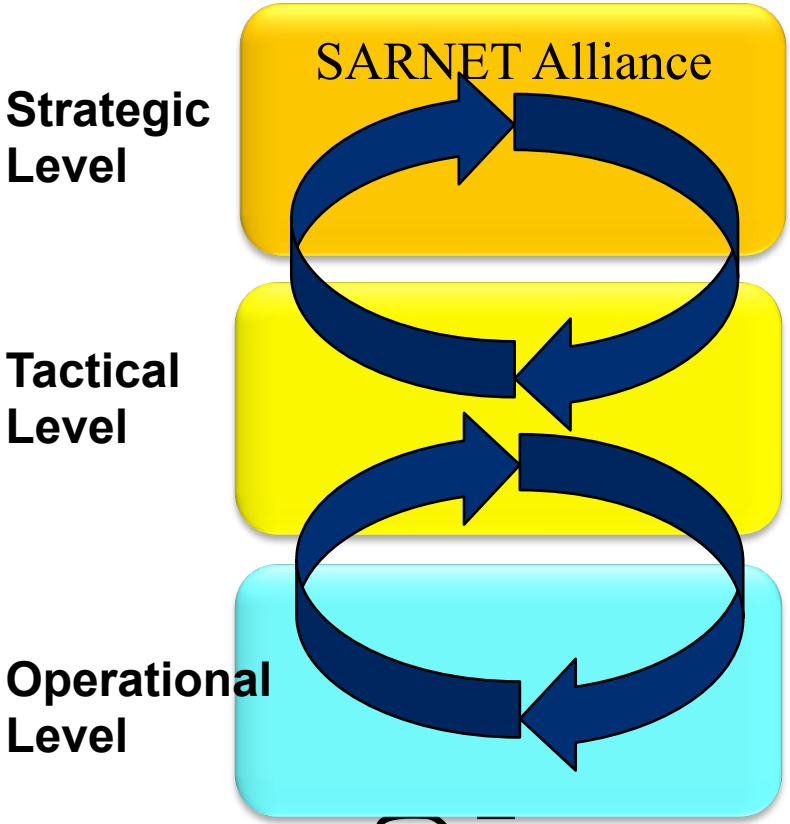
Can we create networks that self detect attacks and are able to autonomously react/ heal?

Is network programmability a step towards digital sovereignty?

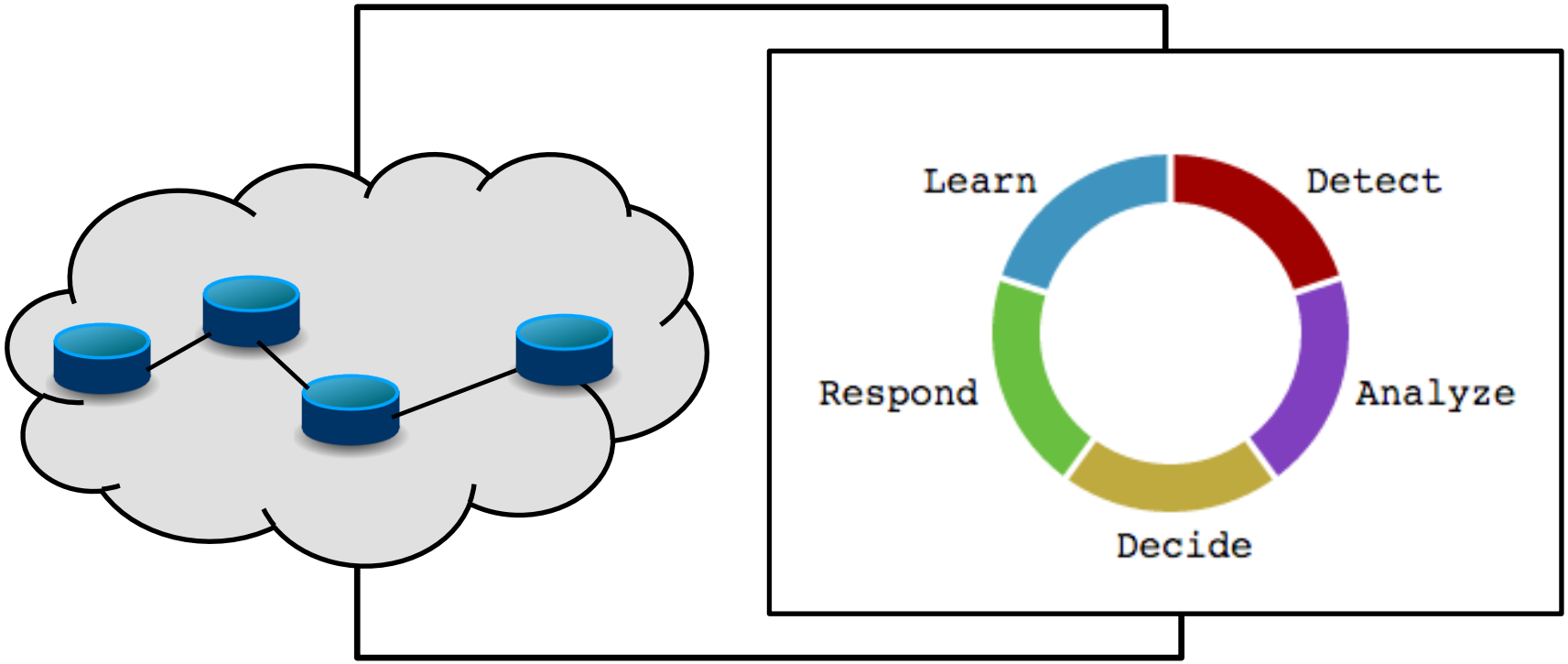
Is network programmability a step toward more control?

SARNET?
Secure Autonomous Response networks

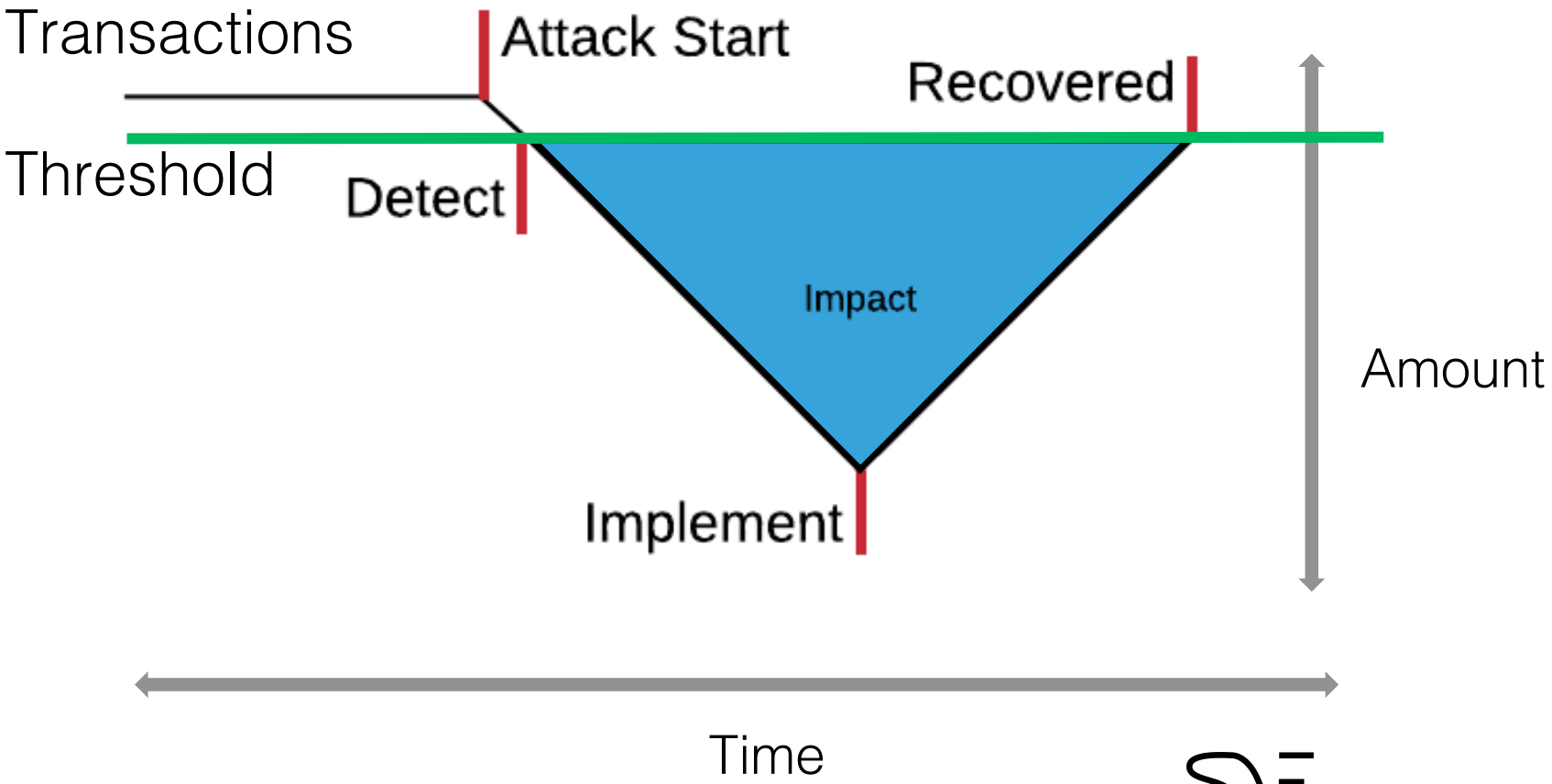




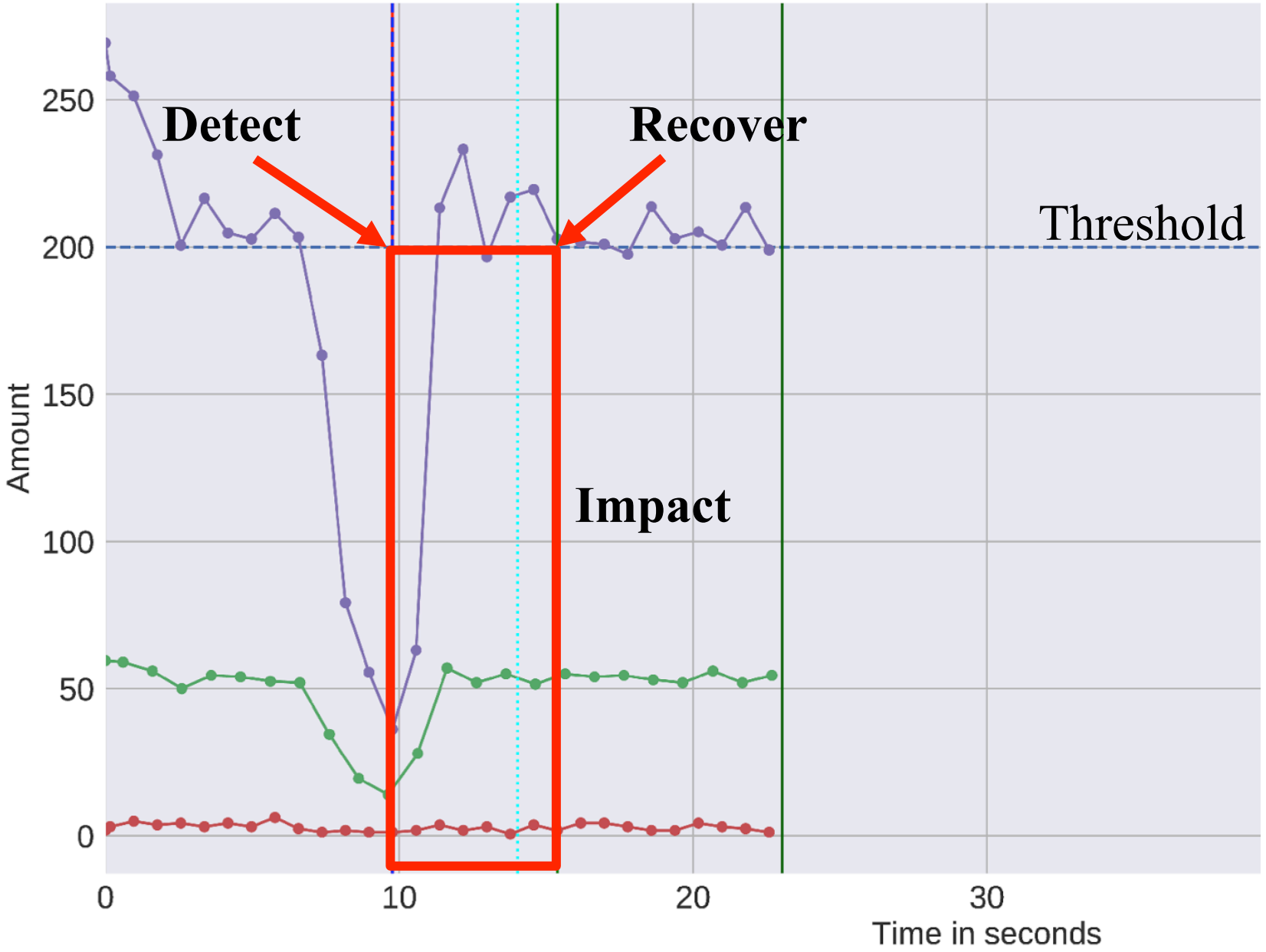
Control loop



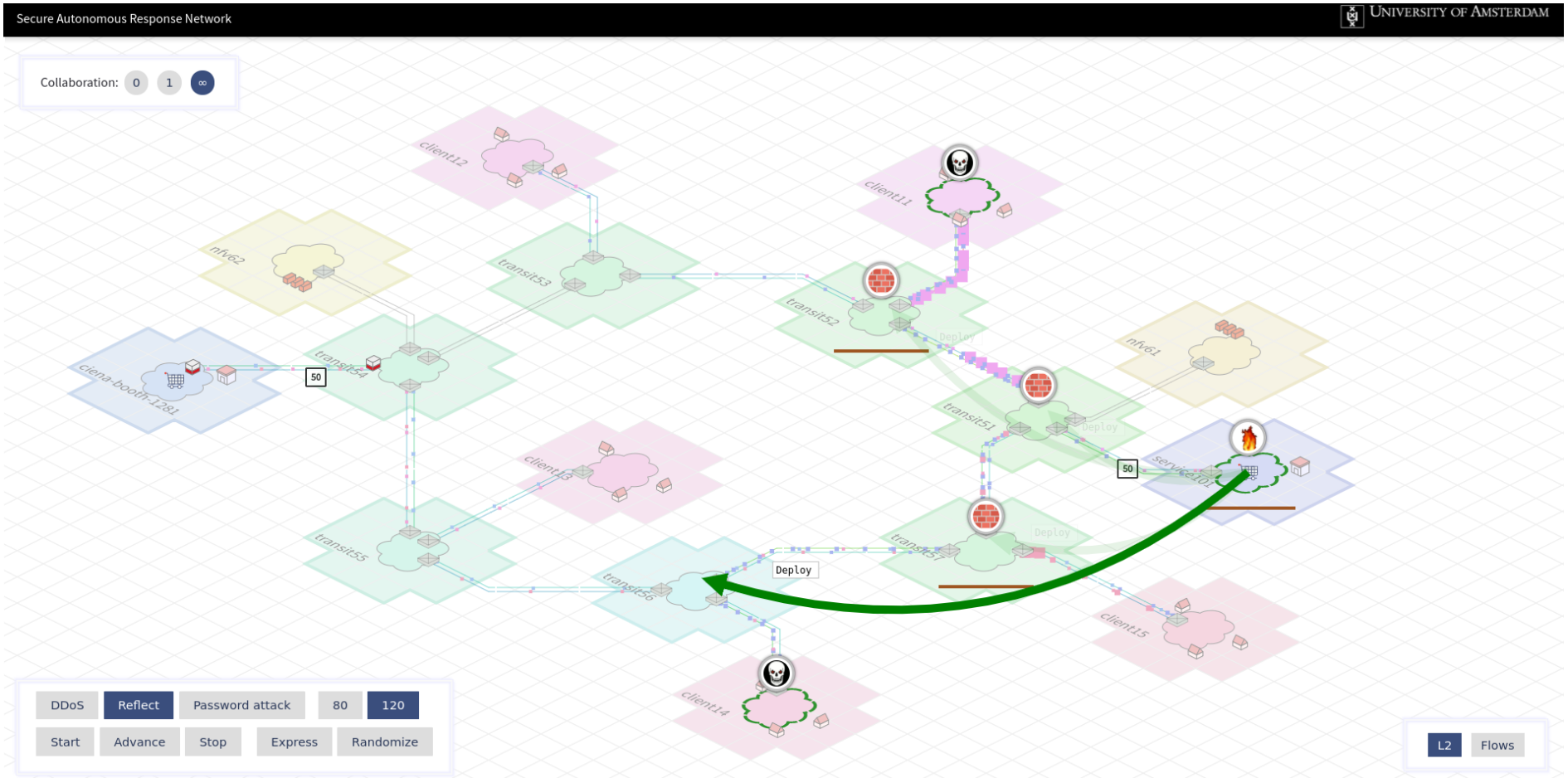
Impact


Transactions
Attack Start
Recovered
Threshold
Detect
Impact
Amount
Implement
Time

Example: DDos attack



Multi-domain

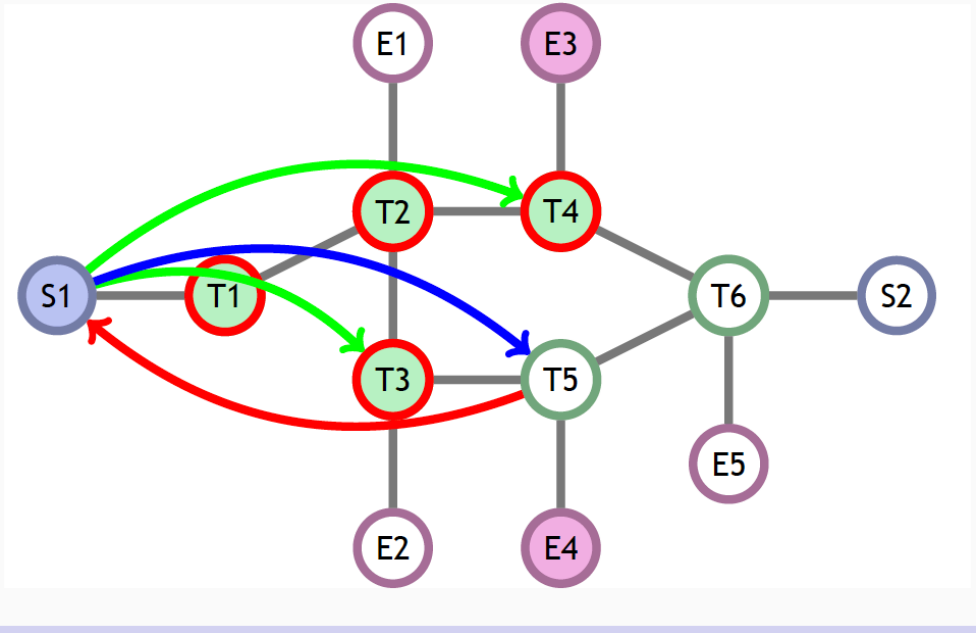


Defense approaches

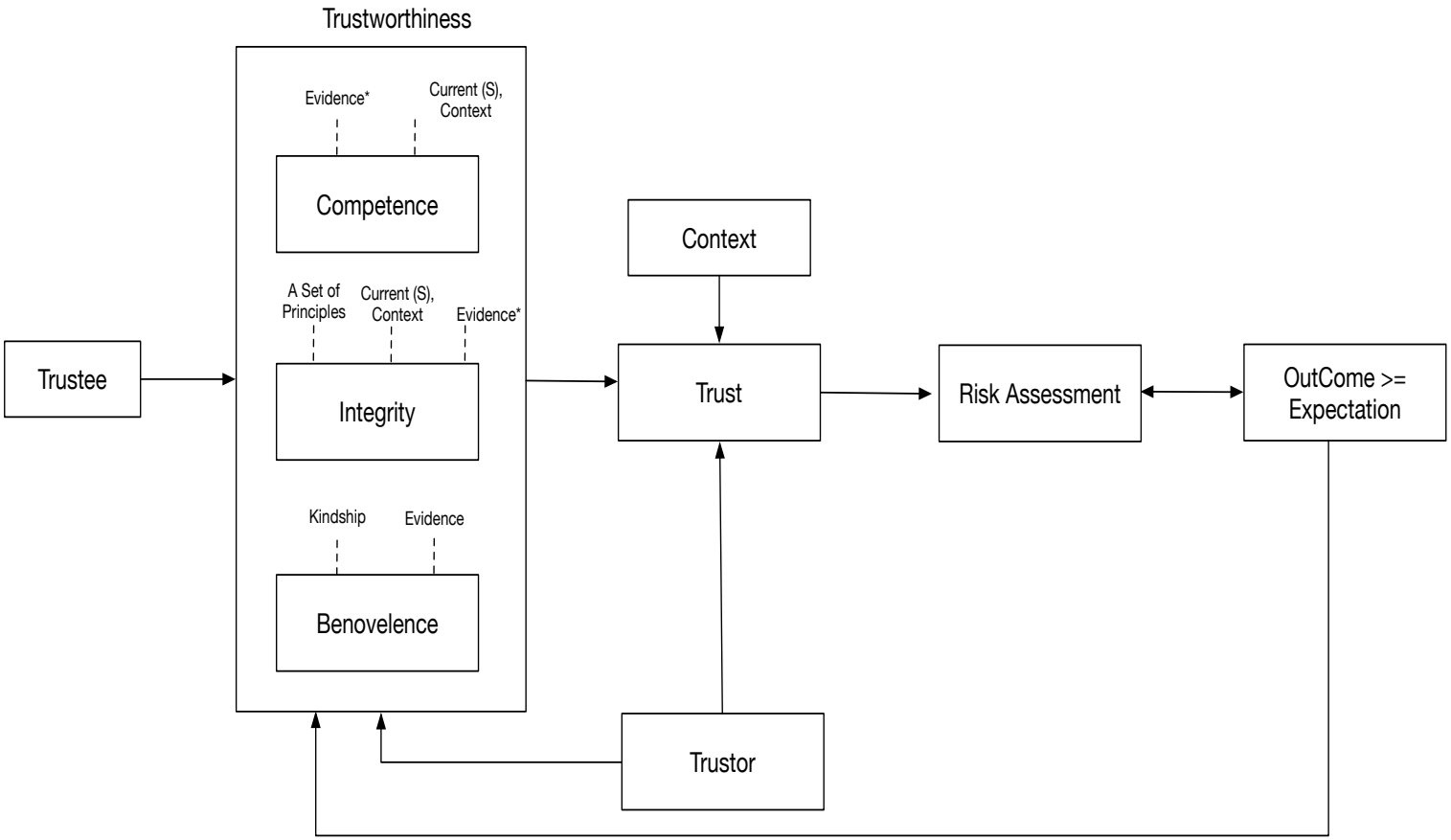
Invoking a multi domain defense can be done in multiple ways.

We look at three of them:

- Blocking immediately at all members.
- Blocking at members close to victims.
- Blocking immediately, evaluate, block again.



Trust framework



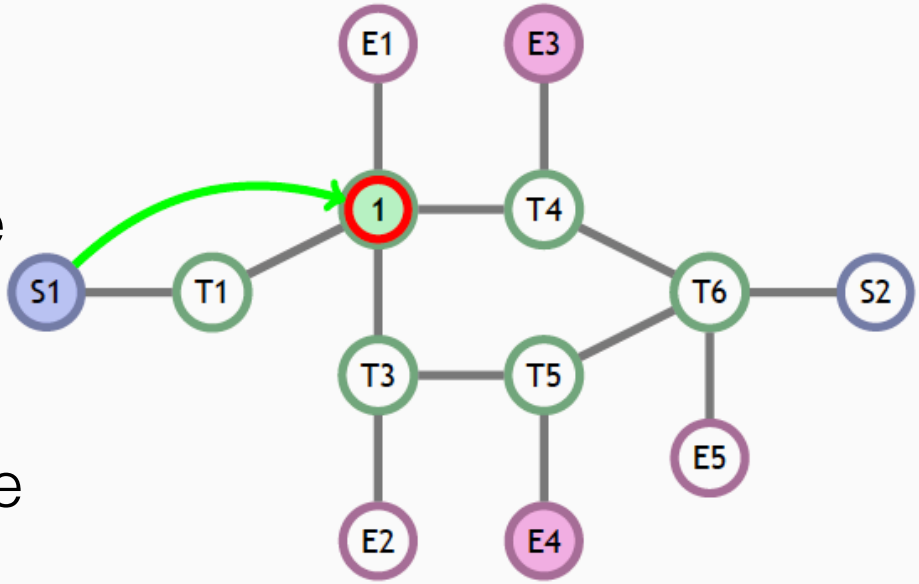
Trustworthiness factors

“x” expects “y” to do “t” and “y” will not exploit vulnerabilities of “x” when “y” faced with the opportunity to do so. Therefore, ``y" has to exhibit:

- demonstrate **competence** related to the potential ability of the evaluated entity to do a given task,
- act accordingly to **fulfill** the **commitments** even when acting on them is not in self-interest and accept the consequences, and
- **do good** and act out of kindness even if unforeseen contingencies arise.

Benevolence based approach

- Assume integrity of alliance members (for now)
- Filter nodes on competence to perform task ‘t‘
- Rank nodes on benevolence
- Ask node with highest benevolence



SARNET project

More information?

https://sarnet.uvalight.net

UNIVERSITEIT VAN AMSTERDAM

System and Network
Engineering