CRITIS '08

Information Infrastructure Protection by Technology driven Policy

Semir Daskapan, Jolien Ubacht, Wim Vree

Delft University of Technology
Technology, Policy and Management, Netherlands

The paradox

- **A law in engineering says**
  - **The larger the chain of interconnected systems is, the more complexity, the lower manageability and reliability will be.**
- **We say:**
  - **The larger the chain of interconnected systems is, the more complexity, the lower manageability, but the higher reliability will be.**

Approach

- **Focus** on computer infrastructures (CI's) as *critical infrastructures*
  - A *critical infrastructure* refers here to the chain of systems, whose failure might cause high direct and/or indirect social, economical or ecological damage.

- **Method**: CI's regarded as *Complex Adaptive Systems* (CAS's)
  - A CAS is a collection of interdependent rule-following agents with interactions resulting in system-wide patterns across the group and allowing it as a whole to undergo spontaneous self-organization.

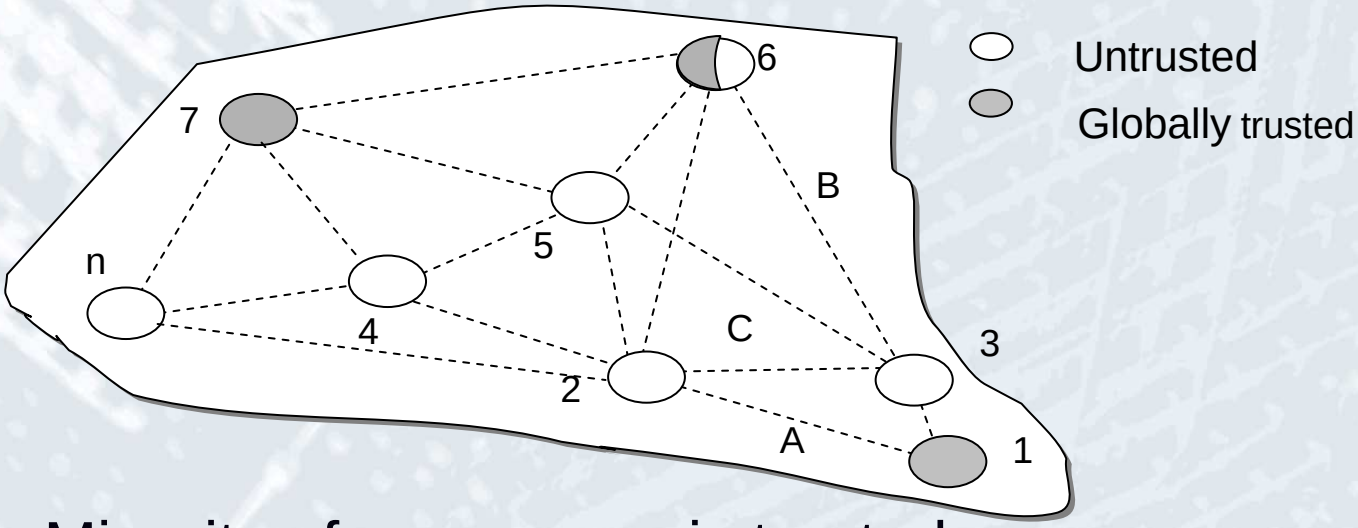
- **Claim 1**: Complexity as a threat to reliability is the solution itself
- **Claim 2**: governments should stimulate the critical CI providers to use a CAS approach when (re)engineering their infrastructure.
- **Underpin**: 3 cases: Self-healing trust, self-healing security, self-healing Internet.

Applying CAS

- A matter of the right assumptions about the knowledge and behavior of the individual agents
- and the right instruction set for each agent
- will lead to emergent behavior, adaptation, specialization, dynamic change, decentralization and cooperation
- When done right the critical CI will heal itself

Case 1. Self- healing trust

- No trusted environment: no secure transactions

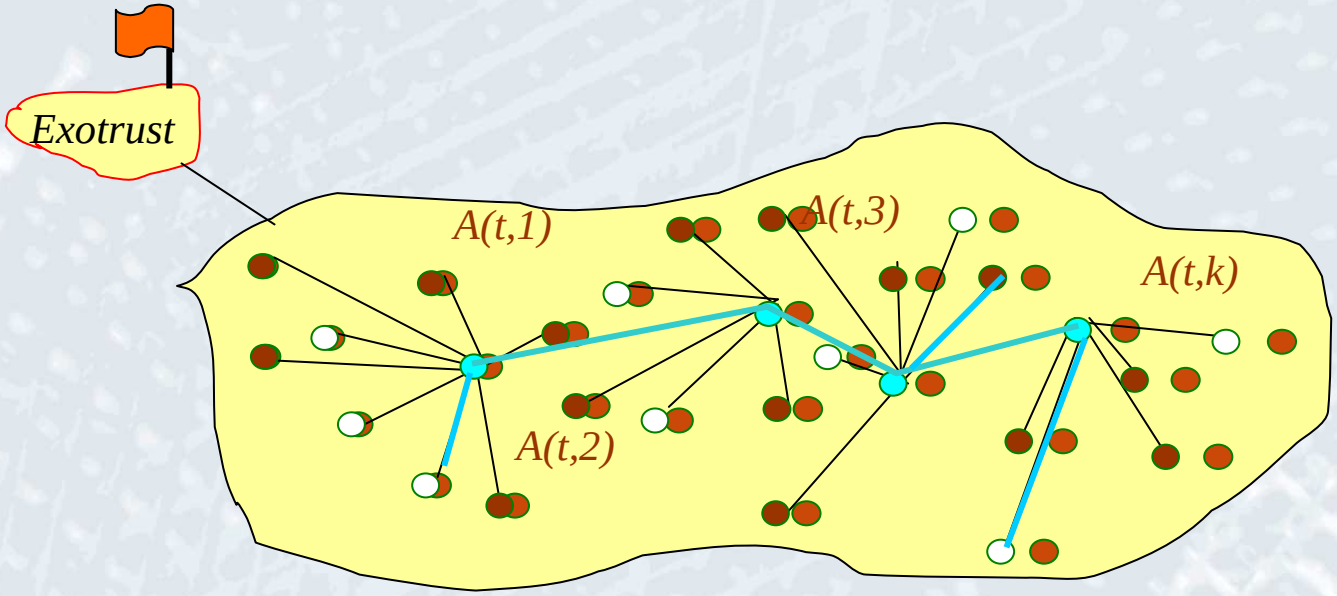


- Minority of processors is trusted
- Trustworthy secure transactions are
  - between 1-3, 2-3, etc not possible.
  - between 1,7(,6?) possible

Case 1: solution

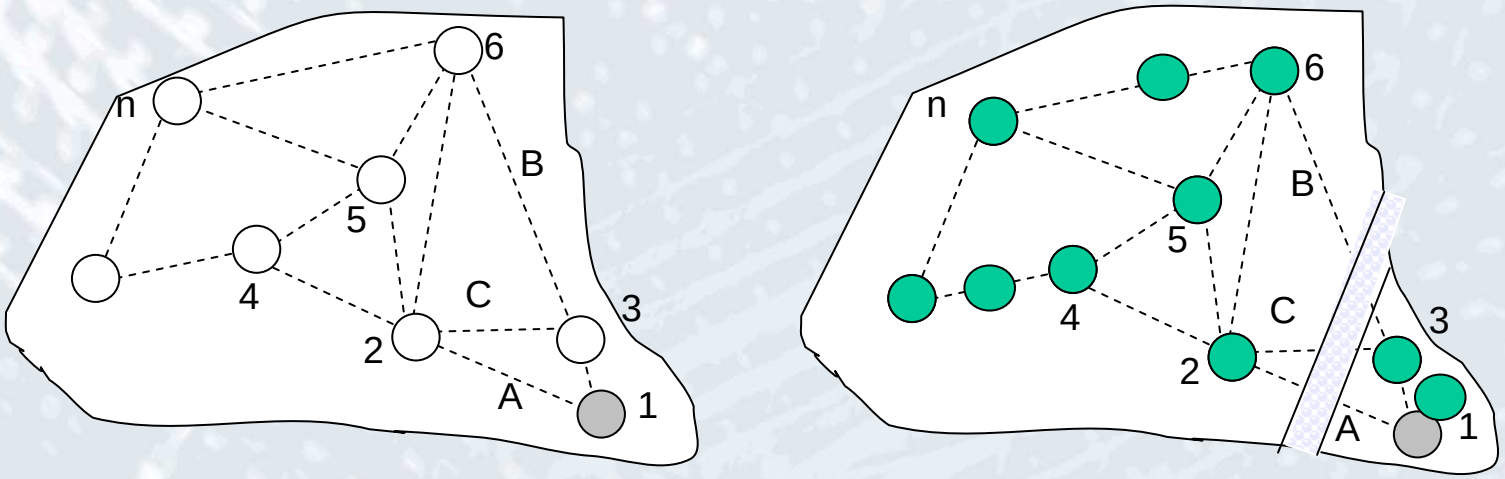
Autonomous and Secure establishment of trust infrastructure

- Anarchy
- Trust assertions
- Elections
- Oligarchy



Case 2. Self- healing security

- **Problem: Reliable security**

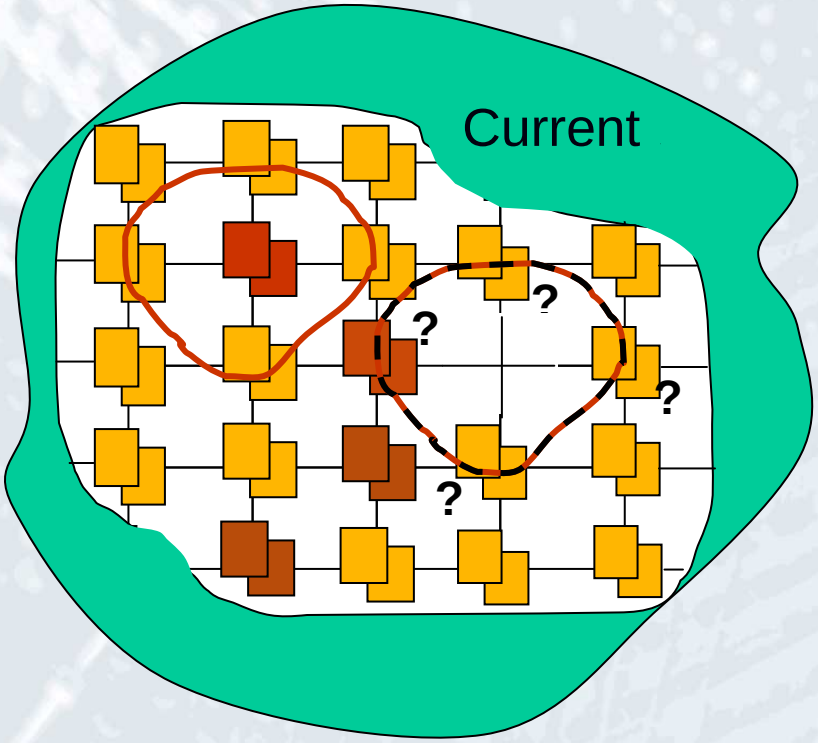


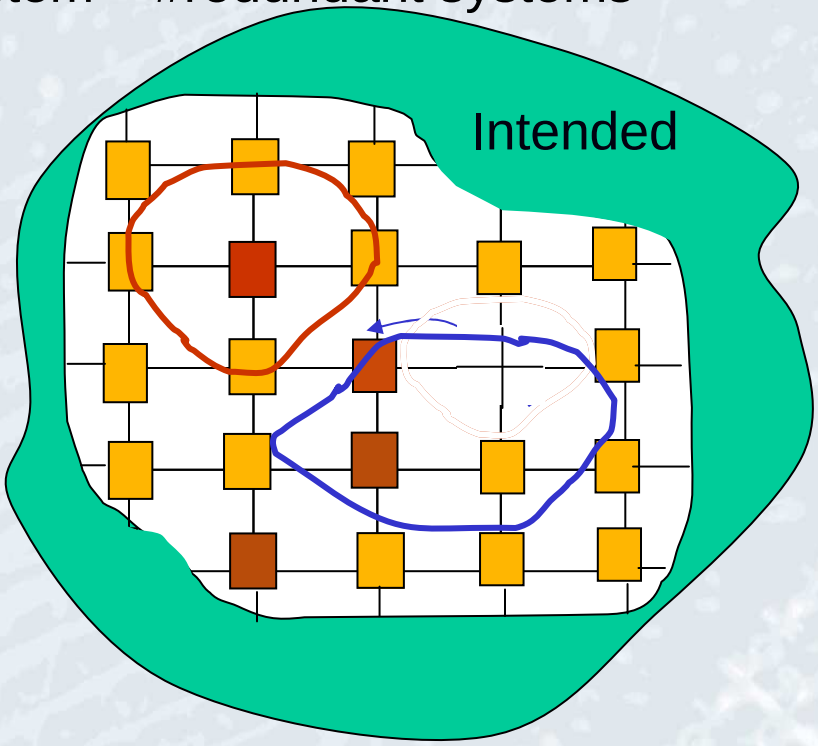
Other processors

Security/trust centre

Case 2: solution = escaping SDC's

- Resource sharing with other critical SDC's
- Survivability = #systems -1,
  - #Systems = 1 main system + #redundant systems





- Survivability = 1
- Survivability = n-1

Case 3: Self- healing Internet

The solution:

- Internet functions as a CAS due to BGP protocol
  - In case of a network failure, this mechanism allows for "routing around the problem“ and heal itself.
  - For increasing number of BGP peers, and thus increasing complexity, the failure tolerance of the overall system increases.
  - Internet functioning as a CAS has, as such, higher reliability with increasing complexity.

- See the dismantling of the KPN/Qwest network
  - resulted in minimal (next slide) disruption of end-to-end connectivity

Case 3: Self- healing Internet

The Problem:

- Routing policies based on commercial considerations of ISP's "pollute" the BGP routing protocol as a CAS.
- Internet becomes more and more de-CASed.
- It is not always able to "heal itself" (in time)
- See sub cases
  - 3.1 Level3 and Cogent: loss of connectivity for parts of the Internet
  - 3.2 KPN/Qwest network: the path from Stockholm to Munich was not re-established on the same day

Role of Governments

- How can they stimulate the adoption of CAS as an engineering method by the private CI market parties?
  - rely on market forces
  - (enforced) co-regulation
  - statutory or formal regulation
  - self-regulation
  - route of standardisation

Conclusion

- Three cases have shown that
  - complexity can be an opportunity to improve reliability
  - of critical infrastructures
  - if CAS is applied correctly
- The role of governments is crucial here
  - either adoption by majority (or main players) of critical CI providers or it is doomed to fail.

http://www.ibm.com

Questions?

semird@tbm.tudelft.nl