# SARNET: Secure Autonomous Response Networks

@ UvA, Amsterdam, Jun 21, 2019

Cees de Laat

**System & Network Engineering**
**University of Amsterdam**

Supported by NWO and C2D grants
SARNET, DL4LD and NWA VWDATA.

# SARNET: Security Autonomous Response with programmable NETworks

Marc Lyonnais, Leon Gommans, Rodney Wilson, Rob Meijer,
Frank Fransen Tom van Engers, Paola Grosso, Gauravdeep Shami, Cees de Laat,
Ameneh Deljoo, Ralph Koning, Ben de Graaff, Gleb Polevoy, Stojan Travanovski.

UNIVERSITY OF AMSTERDAM

AIRFRANCE KLM

ciena

NWO
Netherlands Organisation for Scientific Research

TNO

COMMIT/

# Big Data: real time ICT for logistics
# Data Logistics 4 Logistics Data (dl4ld)

Robert Meijer, TNO, PI, Cees de Laat, UvA, Co-PI, Leon Gommans, KLM

simacan

TNO

AIR FRANCE KLM

ZZ

ORACLE

ciena

THALES

evofenedex

NWO
Netherlands Organisation for Scientific Research

Gemeente
Amsterdam

TRANSFIDES

# SARNET: Security Autonomous Response with programmable NETworks

Marc Lyonnais, Leon Gommans, Rodney Wilson, Rob Meijer,
Frank Fransen Tom van Engers, Paola Grosso, Gauravdeep Shami, Cees de Laat,
Ameneh Deljoo, Ralph Koning, Ben de Graaff, Gleb Polevoy, Stojan Travanovski.

UNIVERSITY OF AMSTERDAM

AIRFRANCE KLM

ciena

NWO Netherlands Organisation for Scientific Research

TNO

COMMIT/

# Big Data: real time ICT for logistics Data Logistics 4 Logistics Data (dl4ld)

Robert Meijer, TNO, PI, Cees de Laat, UvA, Co-PI, Leon Gommans, KLM

simacan

TNO

AIR FRANCE KLM

ORACLE

ciena

THALES

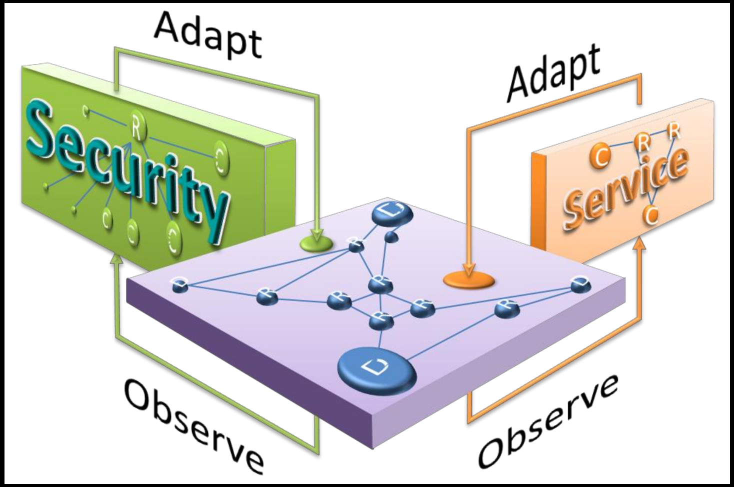
evofenedex

NWO Netherlands Organisation for Scientific Research

Gemeente Amsterdam

TRANSFIDES

# Cyber security program SARNET



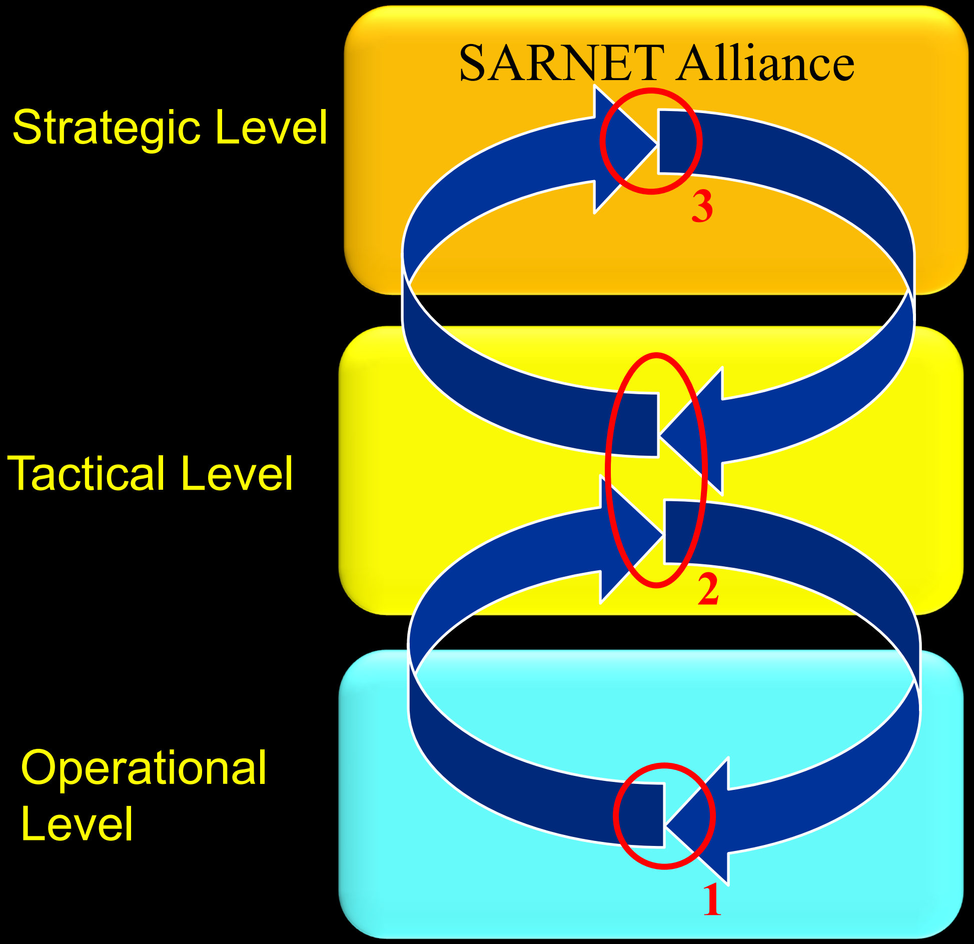
Research goal is to obtain the knowledge to create ICT systems that:

- – model their state (situation)
- – discover by observations and reasoning if and how an attack is developing and calculate the associated risks
- – have the knowledge to calculate the effect of counter measures on states and their risks
- – choose and execute one.

In short, we research the concept of networked computer infrastructures exhibiting SAR: Security Autonomous Response.

# Context & Goal

## Security Autonomous Response NETwork Research

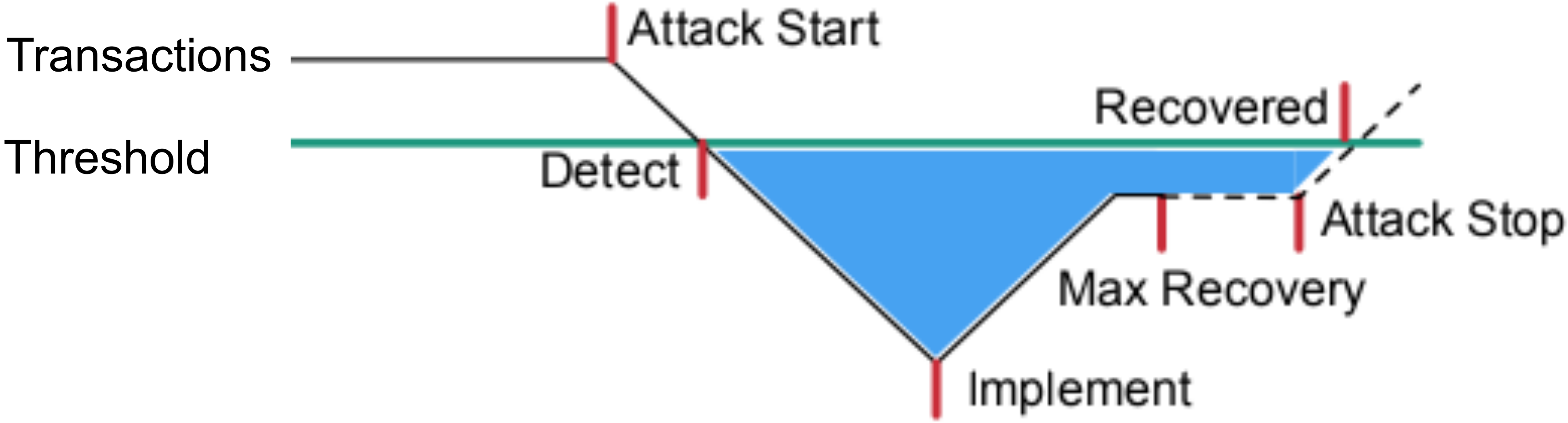


**Ameneh Deljoo (PhD):**
Why create SARNET Alliances? Model autonomous SARNET behaviors to identify risk and benefits for SARNET stakeholders (3)

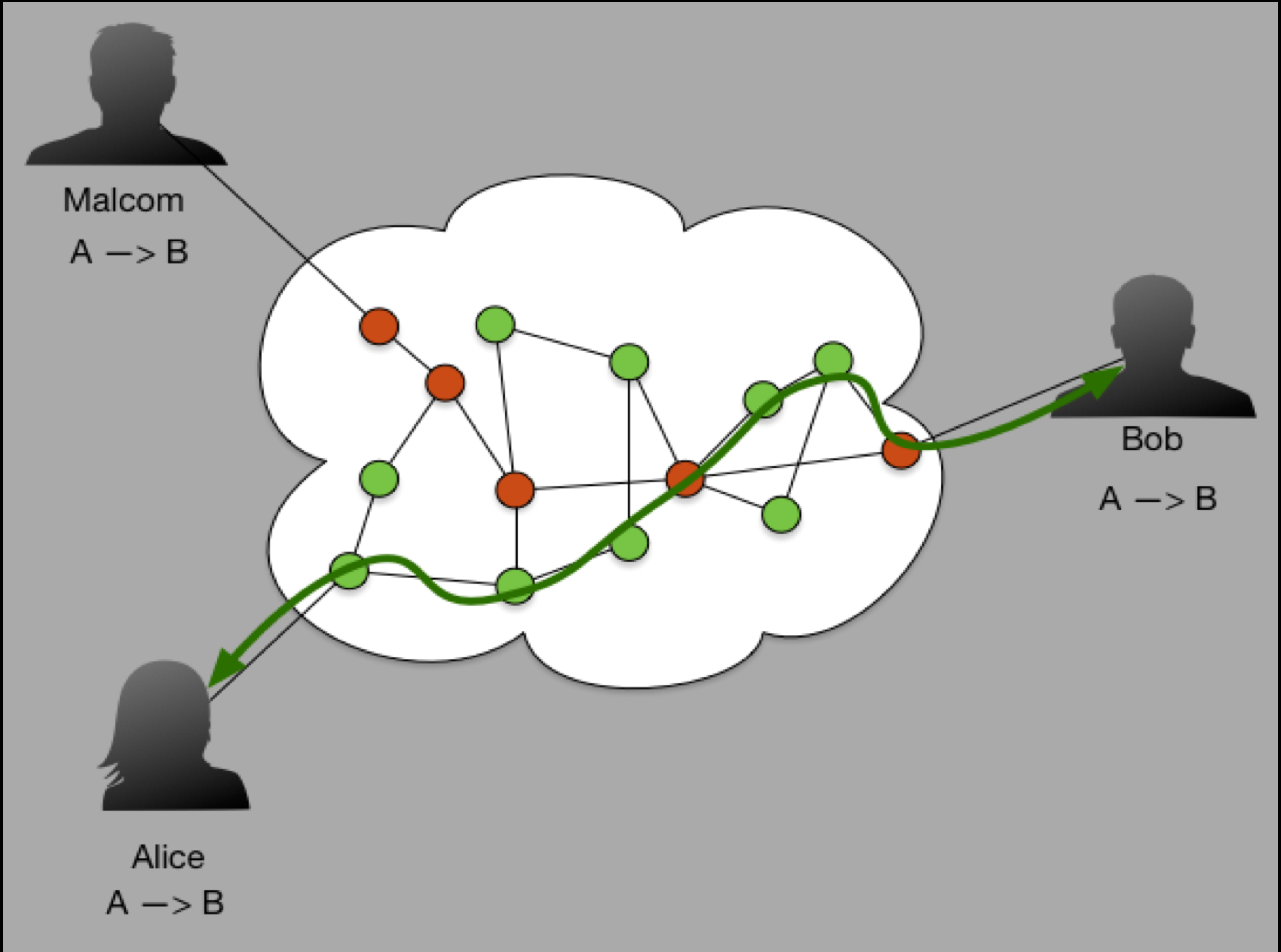
**Gleb Polevoy (PD)**:
Determine best defense scenario against cyberattacks deploying SARNET functions (1) based on security state, KPI information (2) keeping in mind strategic motifs (3).

**Ralph Koning (PhD)**
**Ben de Graaff (SP)**:
1. Design functionalities needed to operate a SARNET using SDN/NFV
2: deliver security state and KPI information (e.g cost)

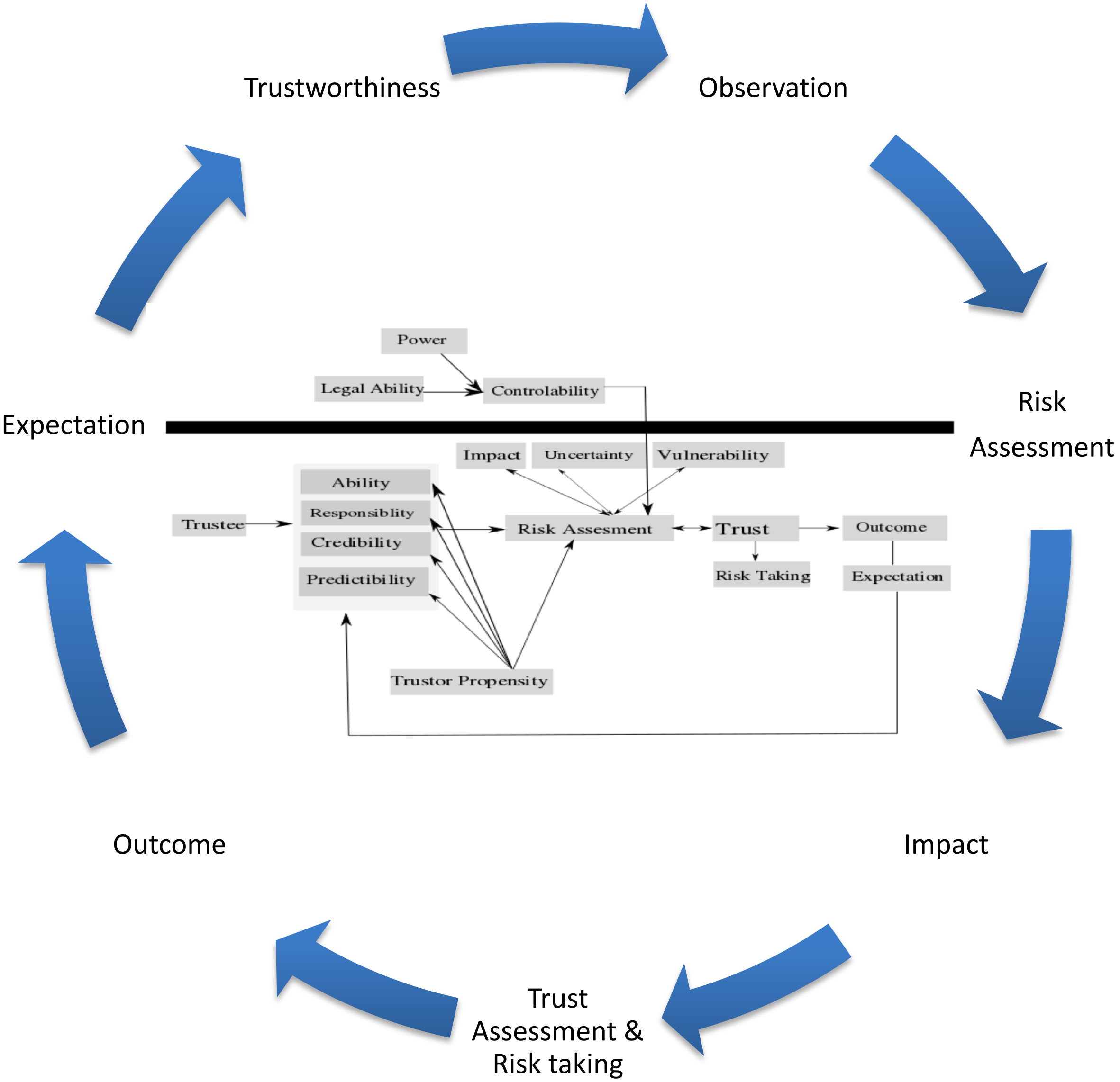
# Effectiveness and Impact



# Example application: Spoofed Network Traffic



# Agent Model evaluating Trust



Trustworthiness

Observation

Risk Assessment

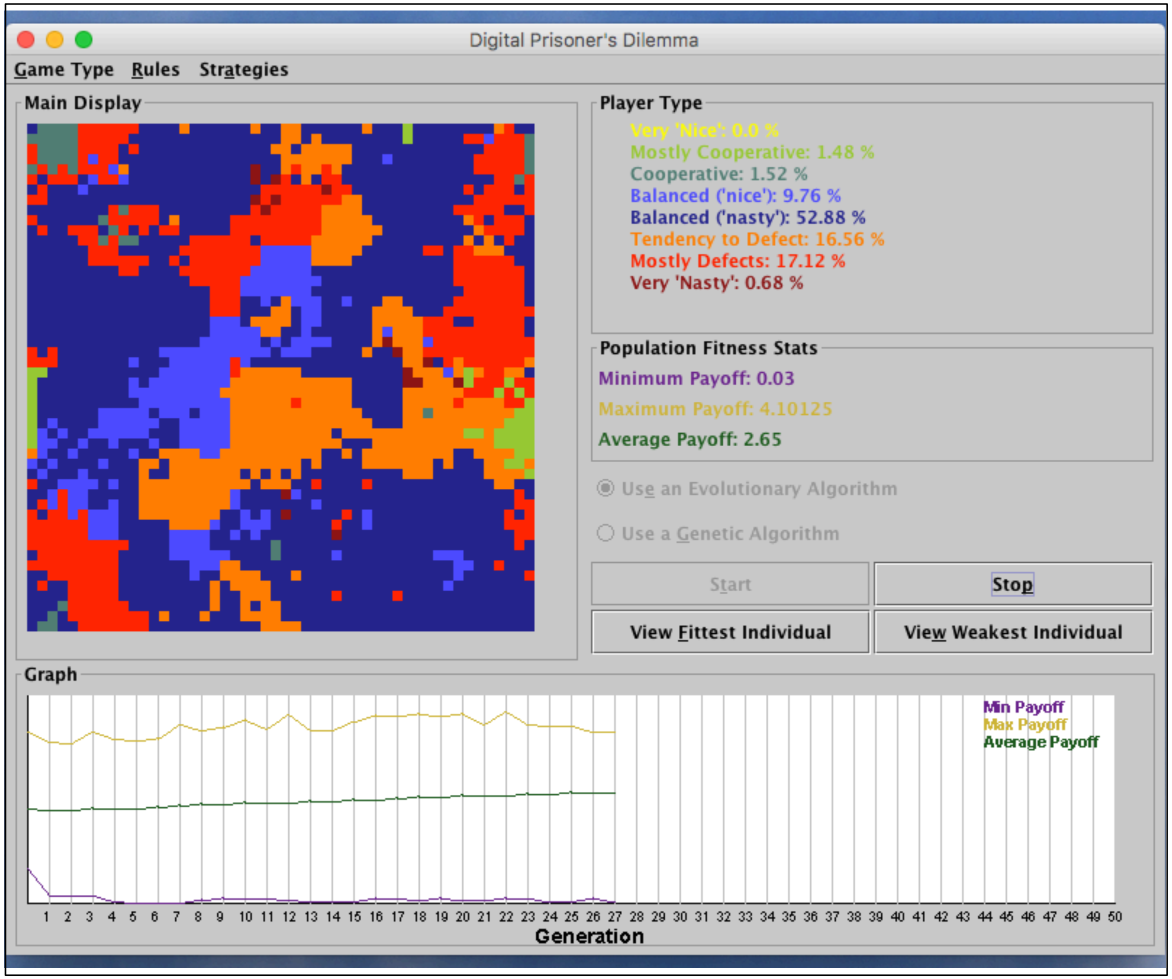
Impact

Trust Assessment & Risk taking

Outcome

Expectation

# First step: Evolutionary Prisoners Dilemma using ABM Simulation



Player Type

Very 'Nice': 0.0 %
Mostly Cooperative: 1.48 %
Cooperative: 1.52 %
Balanced ('nice'): 9.76 %
Balanced ('nasty'): 52.88 %
Tendency to Defect: 16.56 %
Mostly Defects: 17.12 %
Very 'Nasty': 0.68 %

Population Fitness Stats

Minimum Payoff: 0.03

Maximum Payoff: 4.10125

Average Payoff: 2.65

● Use an Evolutionary Algorithm

○ Use a Genetic Algorithm

Agents choose from different strategies:

- Collaborate
- Defect
- During simulation: Agents predict next behavior of neighboring agents learned from observing past behavior.

Simulation observes tendency to maximize individual welfare instead of helping the group.

This type of simulation will be base to simulate more complex collaborations of autonomous organizations.

*Research performed by Ameneh Deljoo, PhD candidate University of Amsterdam.*

# Experiment outcomes
# Note, this was in 2005 at SC and igrid2005!

We have demonstrated seamless, live migration of VMs over WAN

For this, we have realized a network service that

- Exhibits predictable behavior; tracks endpoints
- Flex bandwidth upon request by credited applications
- Doesn’t require peak provisioning of network resources

Pipelining bounds the downtime in spite of high RTTs

- San Diego – Amsterdam, 1GE, RTT = 200 msec, downtime <= 1 sec
- Back to back, 1GE, RTT = 0.2-0.5 msec, downtime = ~0.2 sec*
- **Clark et al. NSDI 05 paper. Different workloads*

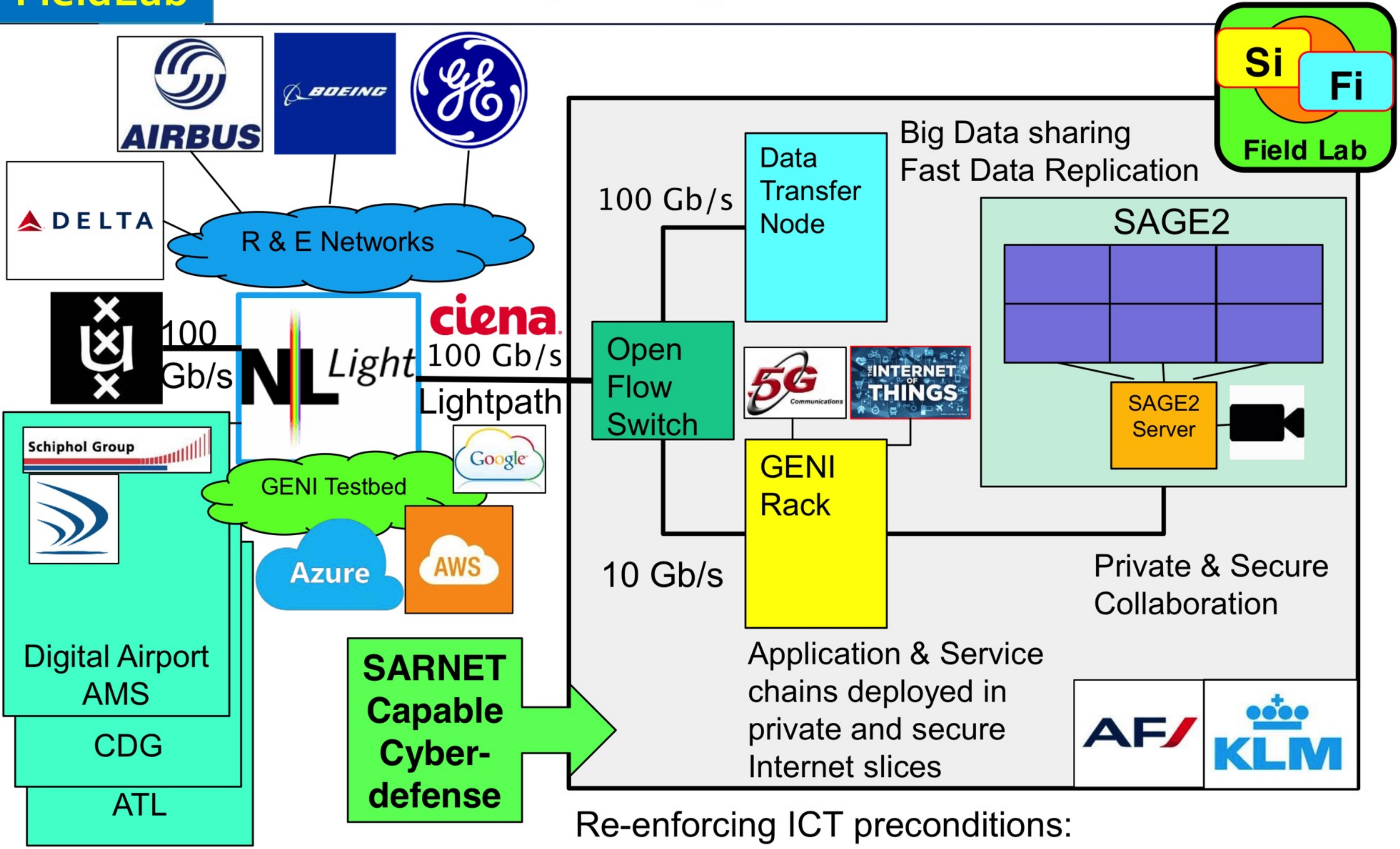
VM + Lightpaths across MAN/WAN are deemed a powerful and general alternative to RPC, GRAM approaches

We believe it’s a representative instance of active cpu+data+net orchestration

F. Travostino, P. Daspit, L. Gommans, C. Jog, C.T.A.M. de Laat, J. Mambretti, I. Monga, B. van Oudenaarde, S. Raghunath and P.Y. Wang, "Seamless Live Migration of Virtual Machines over the MAN/WAN", Future Generation Computer Systems, Volume 22, Issue 8, October 2006, Pages 901-907.

AF/KLM FieldLab

# Ambition to put capabilities into fieldlab

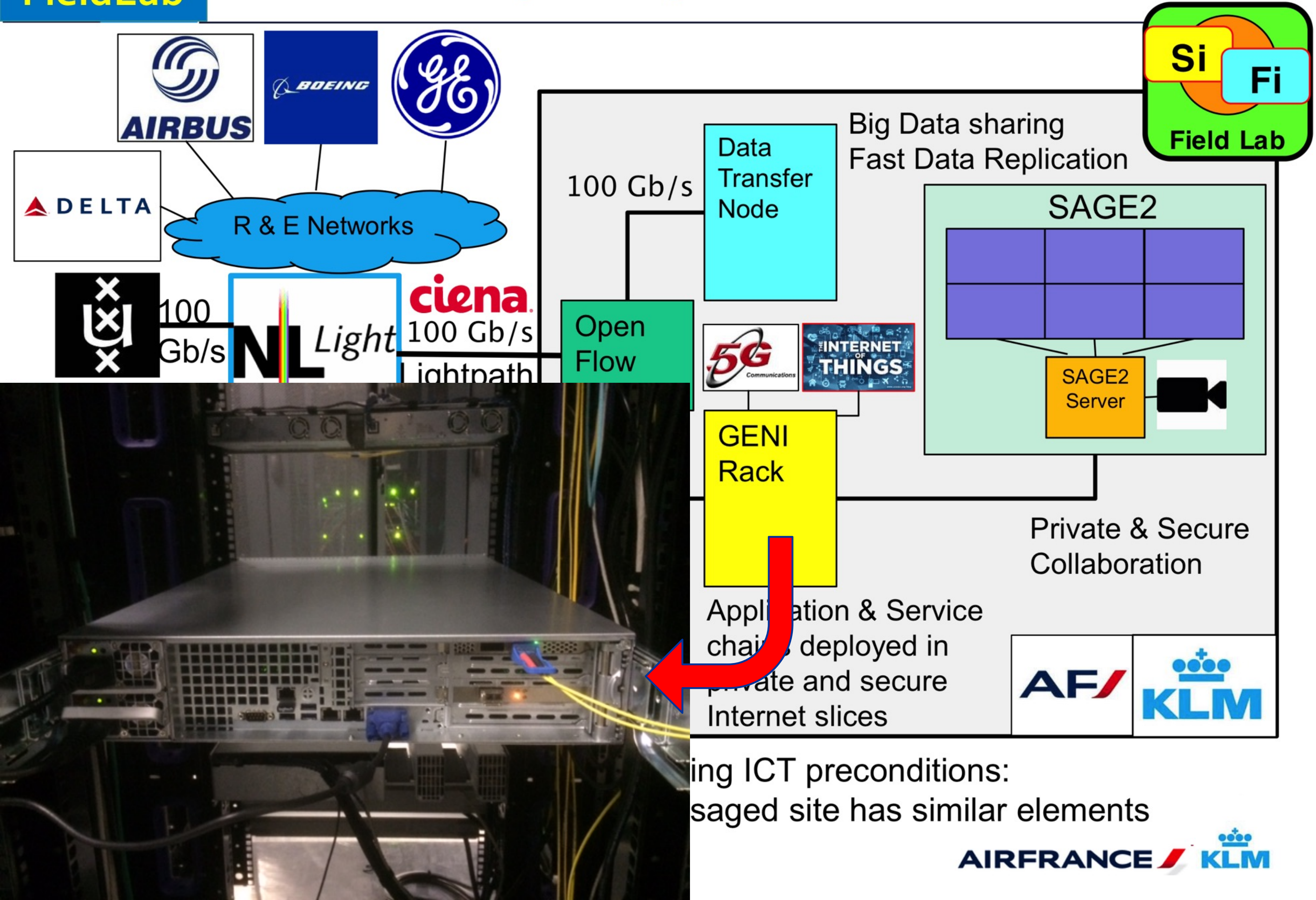


**SARNET Capable Cyber-defense**

Re-enforcing ICT preconditions:
Each envisaged site has similar elements

AF/KLM FieldLab

# Ambition to put capabilities into fieldlab



Big Data sharing
Fast Data Replication

Private & Secure Collaboration

Application & Service chains deployed in private and secure Internet slices

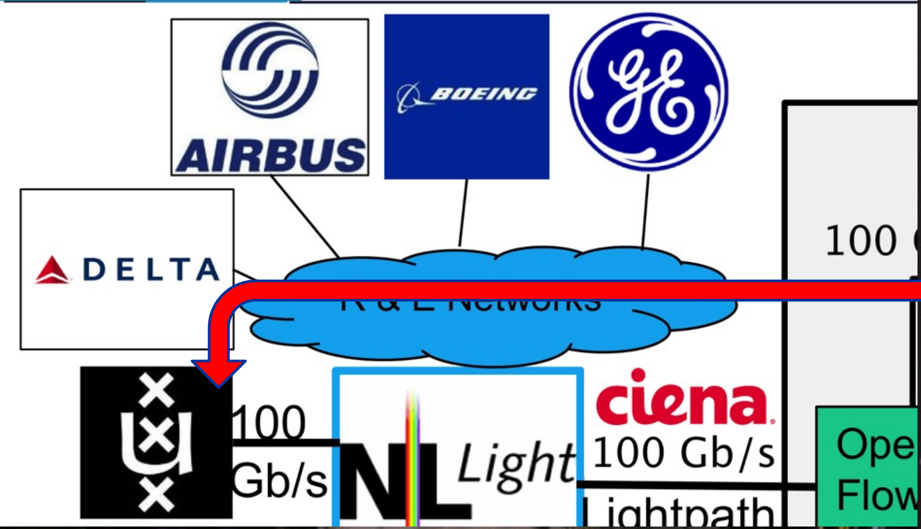
ing ICT preconditions:

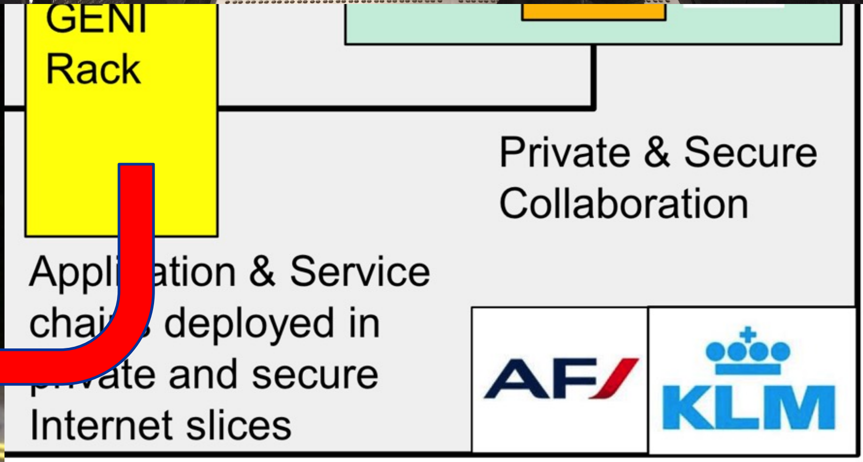
saged site has similar elements

AIRFRANCE KLM

AF/KLM FieldLab

# Ambition to put c





Private & Secure Collaboration

Appl ation & Service chai deployed in ate and secure Internet slices

ing ICT preconditions:

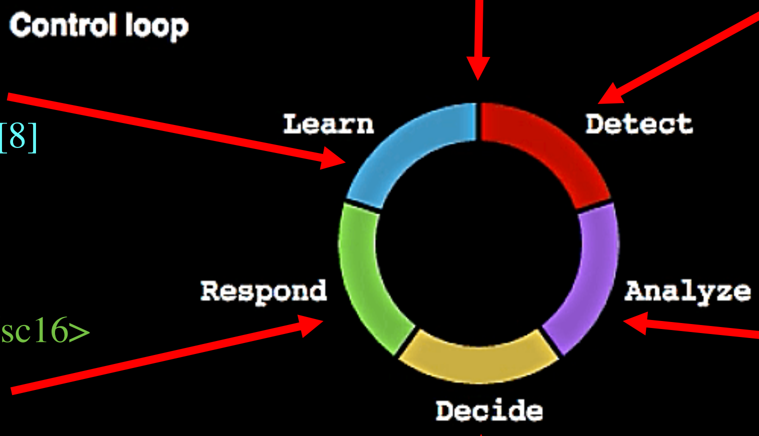
saged site has similar elements

AIRFRANCE KLM

# SARNET Publications (subset)

Laboratory: ExoGeni & PRP
Fieldlab with KLM & CIENA
OSA-Optical Forum Conference paper [1]

SC16 INDIS workshop paper [2]
TNC short paper [4]



IEEE NetSoft paper [5]
efficiency of SDN mitigations [8]

SC16 demo/poster <delaat.net/sc16>
Salt Lake City (UT)
IEEE Sec-Virtnet 2016 paper [3]
Removing Undesirable Flows [6]

SC15 demo/poster <delaat.net/sc16>
Austin (TX)
Sec-Virtnet paper [3]
Computational Trust Model (SCTM) [7]

SC16 demo/poster <delaat.net/sc16>
Salt Lake City (UT)
CoreFlow: Enriching Bro security events [9]

1. Paper: R. Koning, A. Deljoo, S. Trajanovski, B. de Graaff, P. Grosso, L. Gommans, T. van Engers, F. Fransen, R. Meijer, R. Wilson, and C. de Laat, "Enabling E-Science Applications with Dynamic Optical Networks: Secure Autonomous Response Networks ", OSA Optical Fiber Communication Conference and Exposition, 19-23 March 2017, Los Angeles, California.
2. Paper: Ralph Koning, Nick Buraglio, Cees de Laat, Paola Grosso, "CoreFlow: Enriching Bro security events using network traffic monitoring data.", Special section on high-performance networking for distributed data-intensive science, SC16", Future Generation Computer Systems, <accepted for publication>
3. Paper: Ralph Koning, Ben de Graaff, Cees de Laat, Robert Meijer, Paola Grosso, "Analysis of Software Defined Networking defenses against Distributed Denial of Service attacks", The IEEE International Workshop on Security in Virtualized Networks (Sec-VirtNet 2016) at the 2nd IEEE International Conference on Network Softwarization (NetSoft 2016), Seoul Korea, June 10, 2016.
4. Short paper: Nick Buraglio, Ralph Koning, Cees de Laat, Paola Grosso, "Enriching network and security events for event detection", Conference proceedings TNC2017, https://tnc17.geant.org/core/presentation/30.
5. Paper: Ralph Koning, Ben de Graaff, Robert Meijer, Cees de Laat, Paola Grosso, "Measuring the effectiveness of SDN mitigations against cyber attacks", IEEE Conference on Network Softwarization (Netsoft 2017 - SNS 2017), Bologna, Italy, July 3-7, 2017.
6. Paper: Gleb Polevoy, Stojan Trajanovski, Paola Grosso and Cees de Laat, "Removing Undesirable Flows by Edge Deletion.", COCOA'2018 conference, December 15 - 17, 2018, Atlanta, Georgia, USA, Springer-Verlag.
7. Paper: Ameneh Deljoo , Tom van Engers, Leon Gommans, Cees de Laat, “Social Computational Trust Model (SCTM): A Framework to Facilitate Selection of Partners”. In: Proceedings of 2018 IEEE/ACM Innovating the Network for Data-Intensive Science (INDIS), Dallas, TX, USA, 2018
8. Paper: R. Koning, B. de Graaff, G. Polevoy, R. Meijer, C. de Laat, P. Grosso, "Measuring the efficiency of SDN mitigations against attacks on computer infrastructures", Future Generation Computer Systems 91, 144-156.
9. Ralph Koning, Nick Buraglio, Cees de Laat, Paola Grosso, "CoreFlow: Enriching Bro security events using network traffic monitoring data.", Special section on high-performance networking for distributed data-intensive science, SC16", Future Generation Computer Systems

# Q&A

- More information:
  - http://delaat.net/sarnet
  - http://delaat.net/dl4ld