

SARNET: Secure Autonomous Response Networks

@ KLM, Amsterdam, Dec 8, 2017

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.



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



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.



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

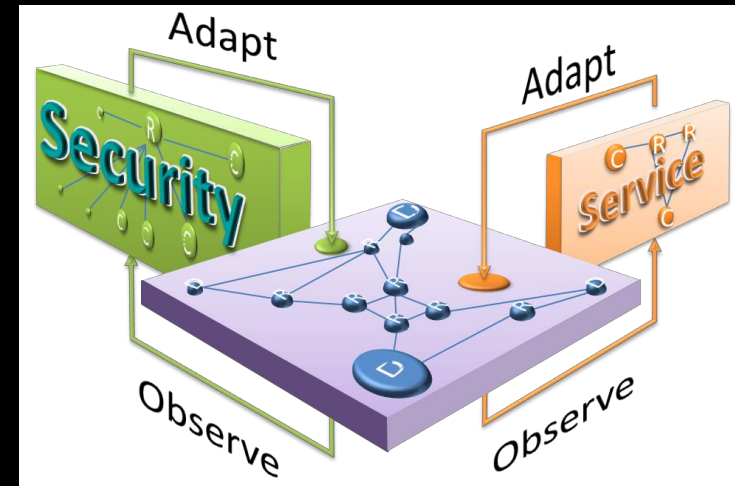
Robert Meijer, TNO, PI, Cees de Laat, UvA, Co-PI, Leon Gommans, KLM



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.

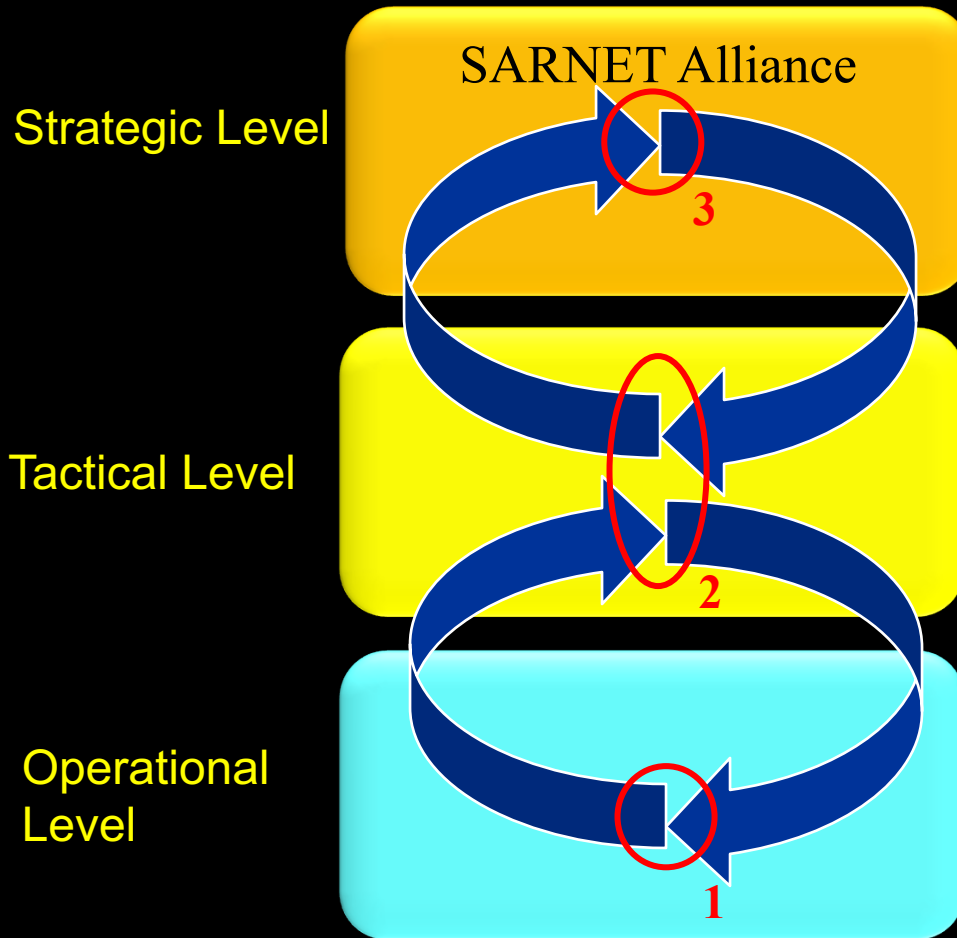


In short, we research the concept of networked computer infrastructures exhibiting SAR: Security Autonomous Response.



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):

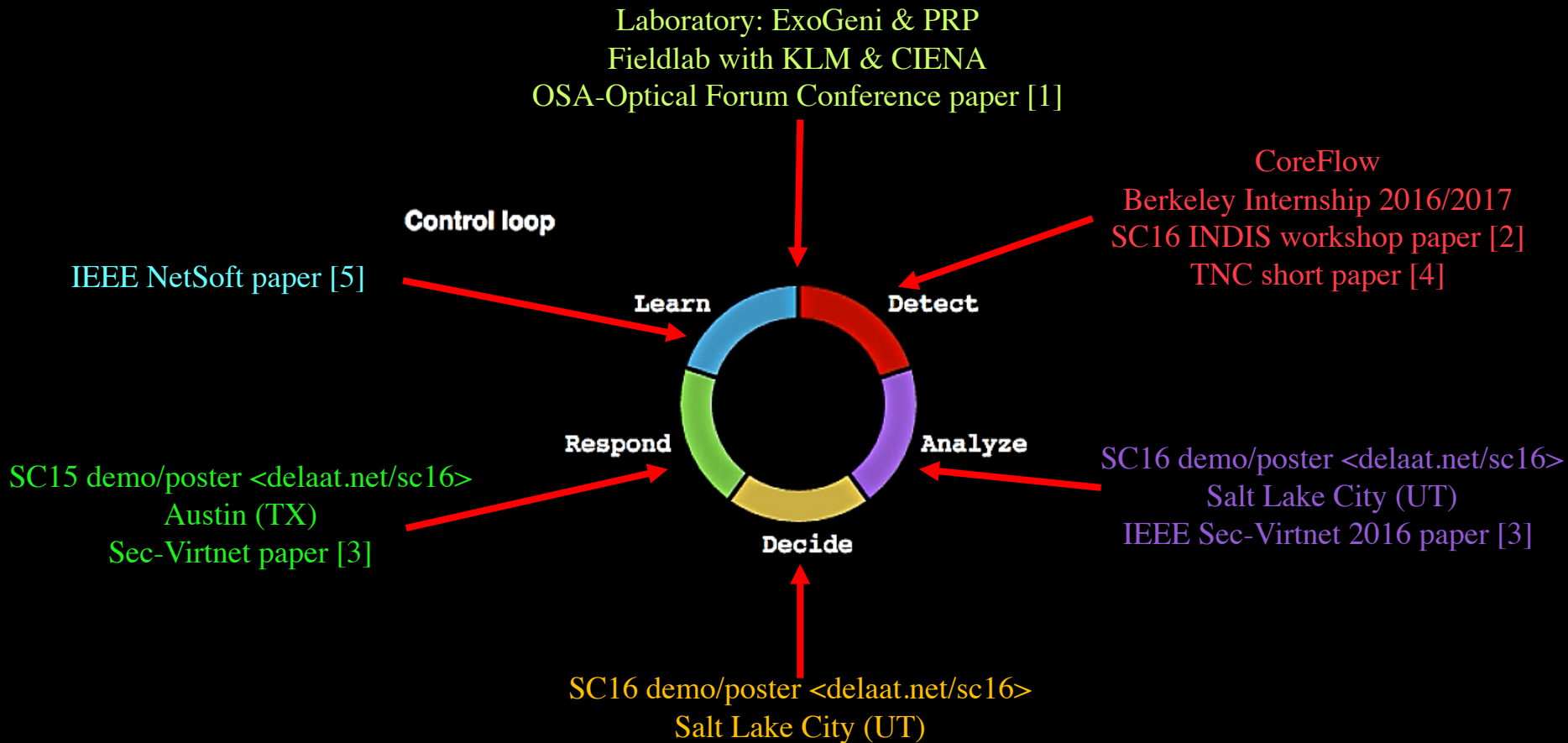
Determine best defense scenario against cyberattacks deploying SARNET functions (1) based on security state, KPI information (2) keeping in mind strategic motifs (3).

Ralph Koning (PhD)

Ben de Graaff (SP):

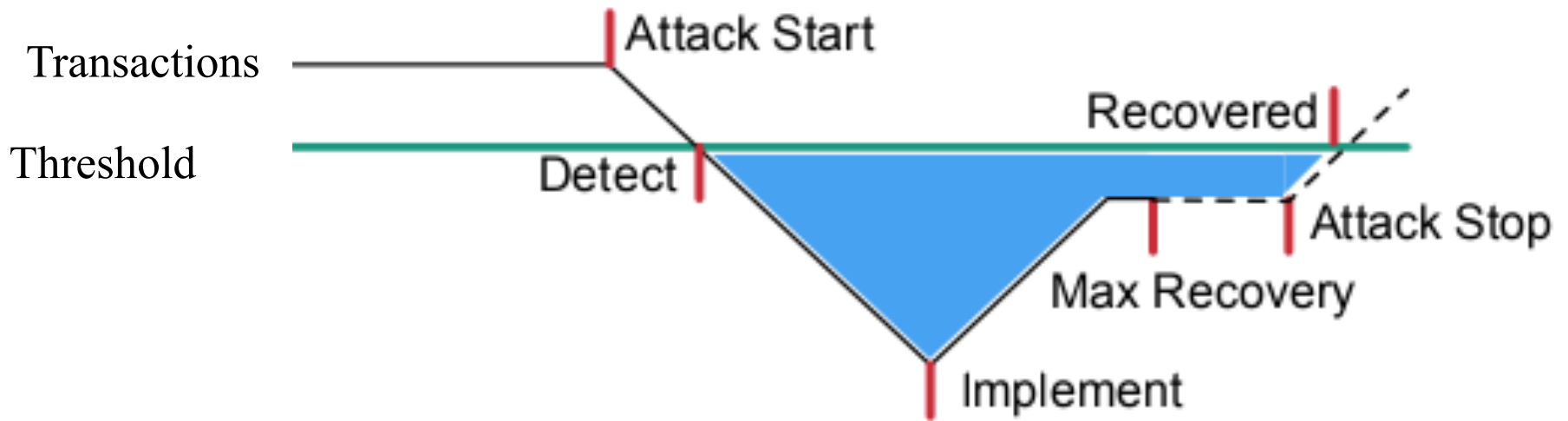
1. Design functionalities needed to operate a SARNET using SDN/NFV
2: deliver security state and KPI information (e.g cost)

Status SARNET Operational Level



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.

Effectiveness and Impact



Scenario

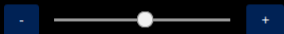


Timeout: 956



SARNET demo

Control loop delay:



By using SDN and containerized NFV, the SARNET agent can resolve network and application level attacks.

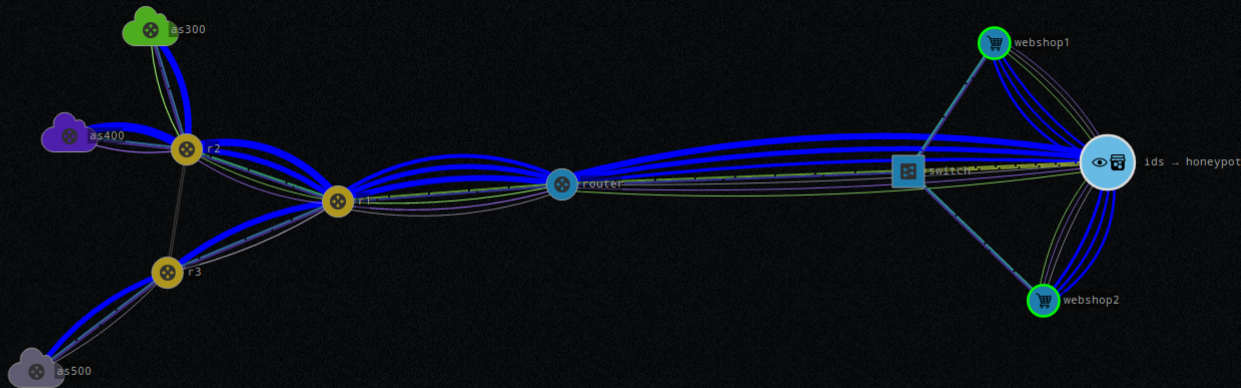
From this screen, you can choose your attack and see the defensive response.

Traffic layers

Toggle the visibility of the traffic layers:

Physical links

Traffic flows



Choose your attack

Start a Distributed Denial of Service attack from all upstream ISP networks:

UDP DDoS

Start a specific attack originating from one of the upstream ISP networks:

Origin: UNSELECTED - CLICK ON A CLOUD

CPU utilization

Password attack

Normal operation

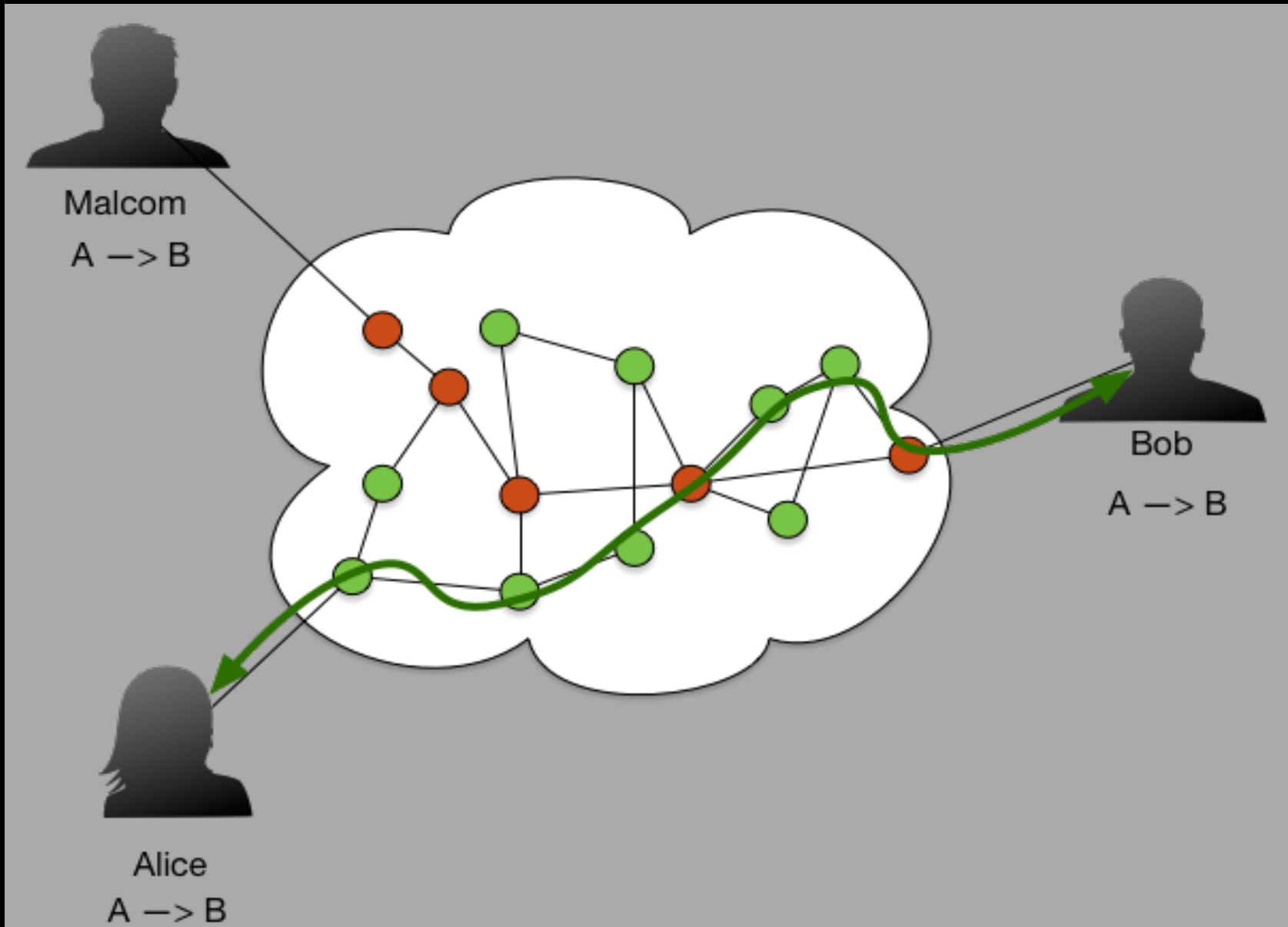
Object information

nfv.services.as100

```
KIND nfv
COMPUTE#DISKIMAGE 8d8d8a23-c112-421b-baba-49383679dc0b#img-nfv
COMPUTE#SPECIFICCE exogeni#XOLarge
EC2#WORKERNODEID uva-nl-w1
REQUEST#HASRESER... request#Active
REQUEST#INDOMAIN uvanlvmsite.rdf#uvanlvmsite/Domain/vm
HONEYPOT.PWS [yamaha enter johnson]
IDS.CPU []
IDS.PW [10.100.4.100 10.100.4.101 10.100.4.102]
NFV-CHAIN [ids honeypot:4.100:4.101:4.102]
CPU-PCT 13
```

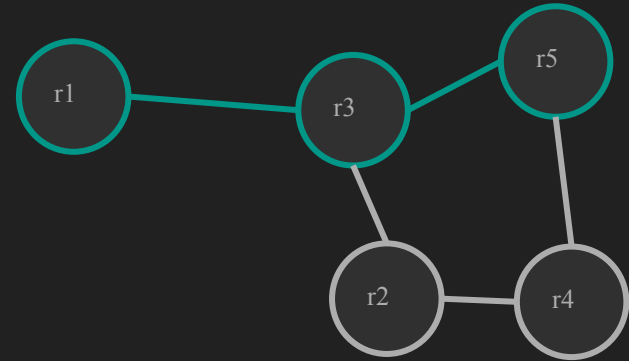

SC16 DEMO SARNET Operational Level

Example application: Spoofed Network Traffic



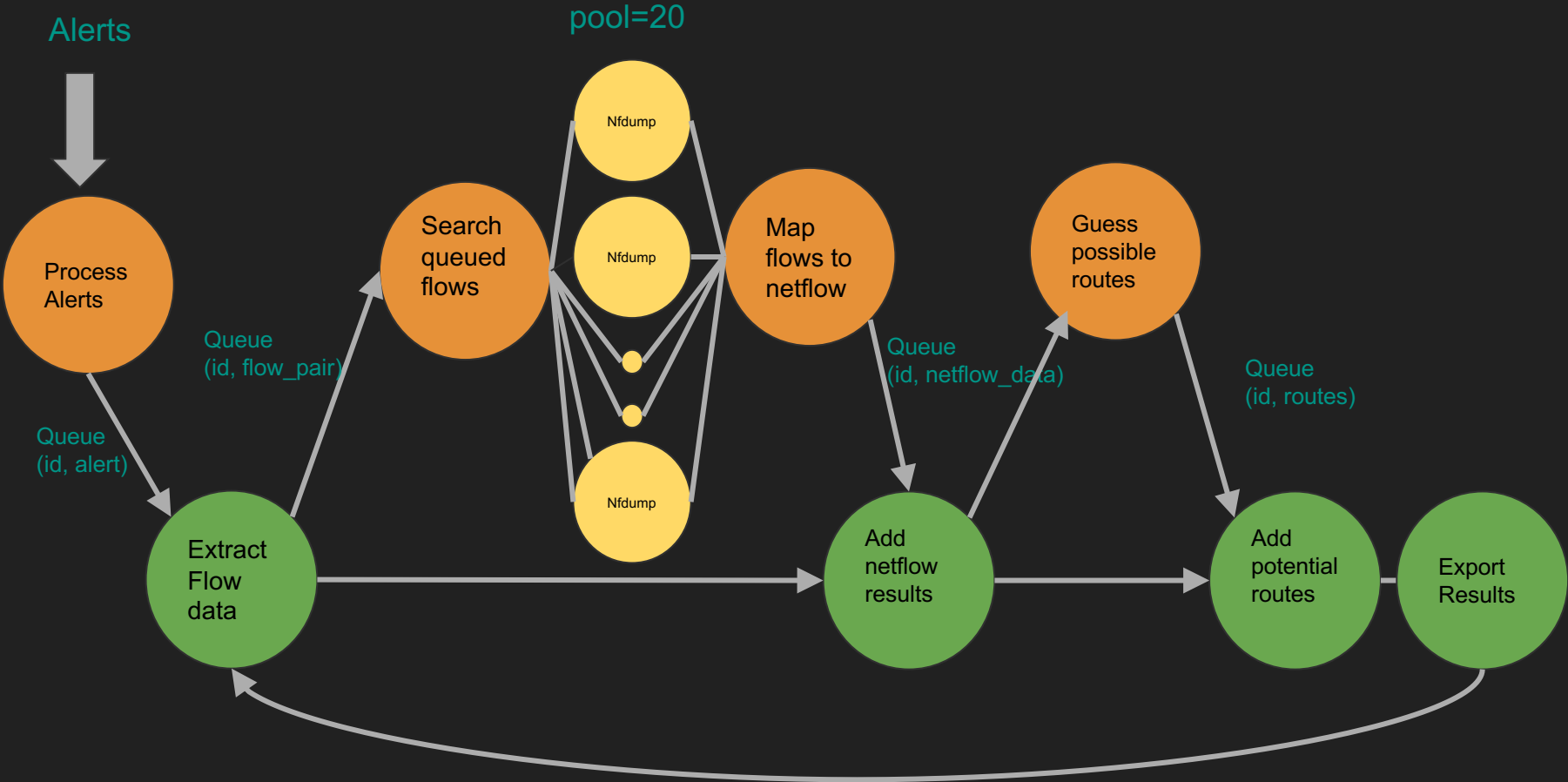
CoreFlow Route estimation algorithm

- It's able to fill in missing routers
- Flow traverse a router multiple times (loops)
- Finds potential 'shortest paths'
- Topology information from OSCARS
- Based on latest topology
- Does not account for policies or metrics



Unordered route:	Get possible routes from r3:	Reverse	Concat	Shortest
r3, r1, r5	r3, r1	r1, r3	r1, r3, r1	r1, r3, r5
	r3, r5	r5, r3	r1, r3, r5	r5, r3, r1
	r3, r2	r2, r3	r1, r3, r2	
	r3, r5, r4	r4, r2, r3	r1, r3, r2, r4	
	r3, r2, r4	r4, r5, r3	r1, r3, r5, r4	
			...	

Current workflow



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.

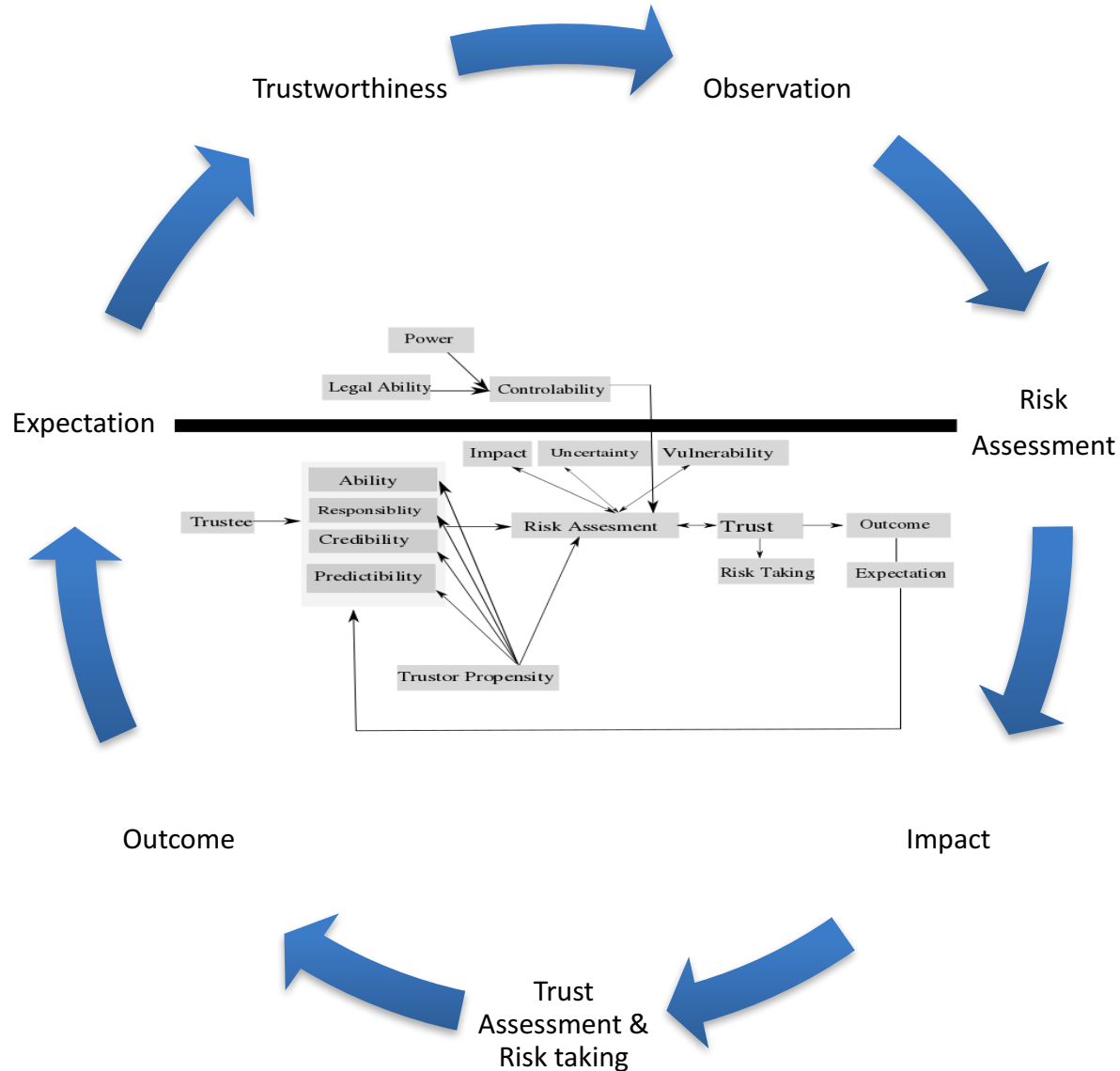
Agent Based Modelling Framework

	Main component
Signal layer	Message / Act
Action layer	Action / Activity
Intentional layer	Intention
Motivational layer	Motive

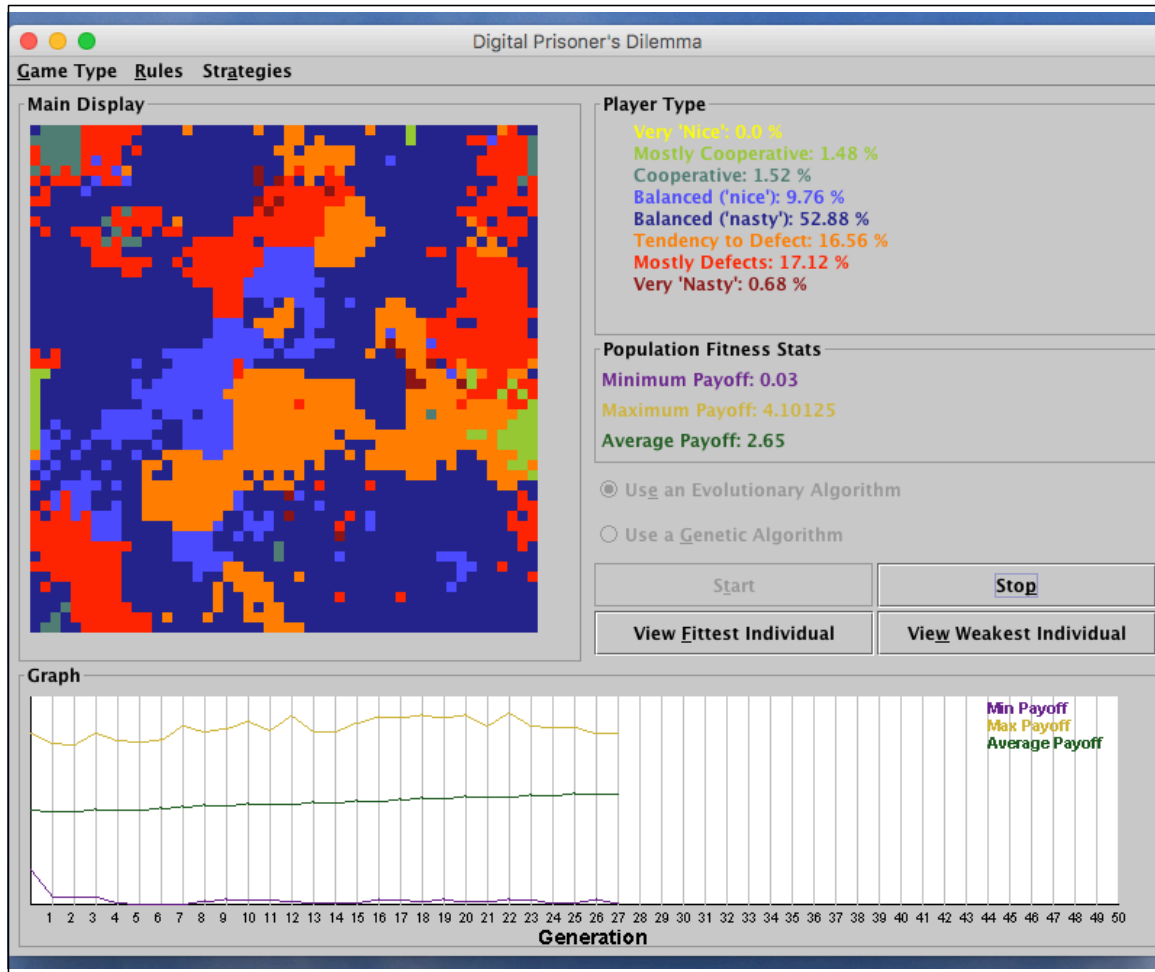
In our model, we refer to four layers of components:

- the signal layer— describes **acts**, side-effects and failures showing outcomes of actions in a topology.
- the action layer—**actions**: performances that bring a certain result,
- the intentional layer—**intentions**: commitments to actions, or to build up intentions,
- the motivational layer—**motives**: events triggering the creation of intentions.

Agent Model evaluating Trust



First step: Evolutionary Prisoners Dilemma using ABM Simulation



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.

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.



AIRFRANCE KLM



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



TNO



AIR FRANCE KLM



ORACLE



THALES



TRANSFIDES

Main problem statement

- Organizations that normally compete have to bring data together to achieve a common goal!
- The shared data may be used for that goal but not for any other!
- Data may have to be processed in untrusted data centers.
 - How to enforce that using modern Cyber Infrastructure?
 - How to organize such alliances?
 - How to translate from strategic via tactical to operational level?
 - What are the different fundamental data infrastructure models to consider?



Big Data Sharing use cases placed in airline context

Global Scale



Aircraft Component Health Monitoring (Big) Data
NWO **CIMPLO** project
4.5 FTE

National Scale



Cargo Logistics Data
(C1) DaL4LoD
(C2) **Secure scalable policy-enforced distributed data Processing**
(using blockchain)

City / regional Scale

Campus / Enterprise Scale

NLIP iShare project



iSHARE
powered by NLIP



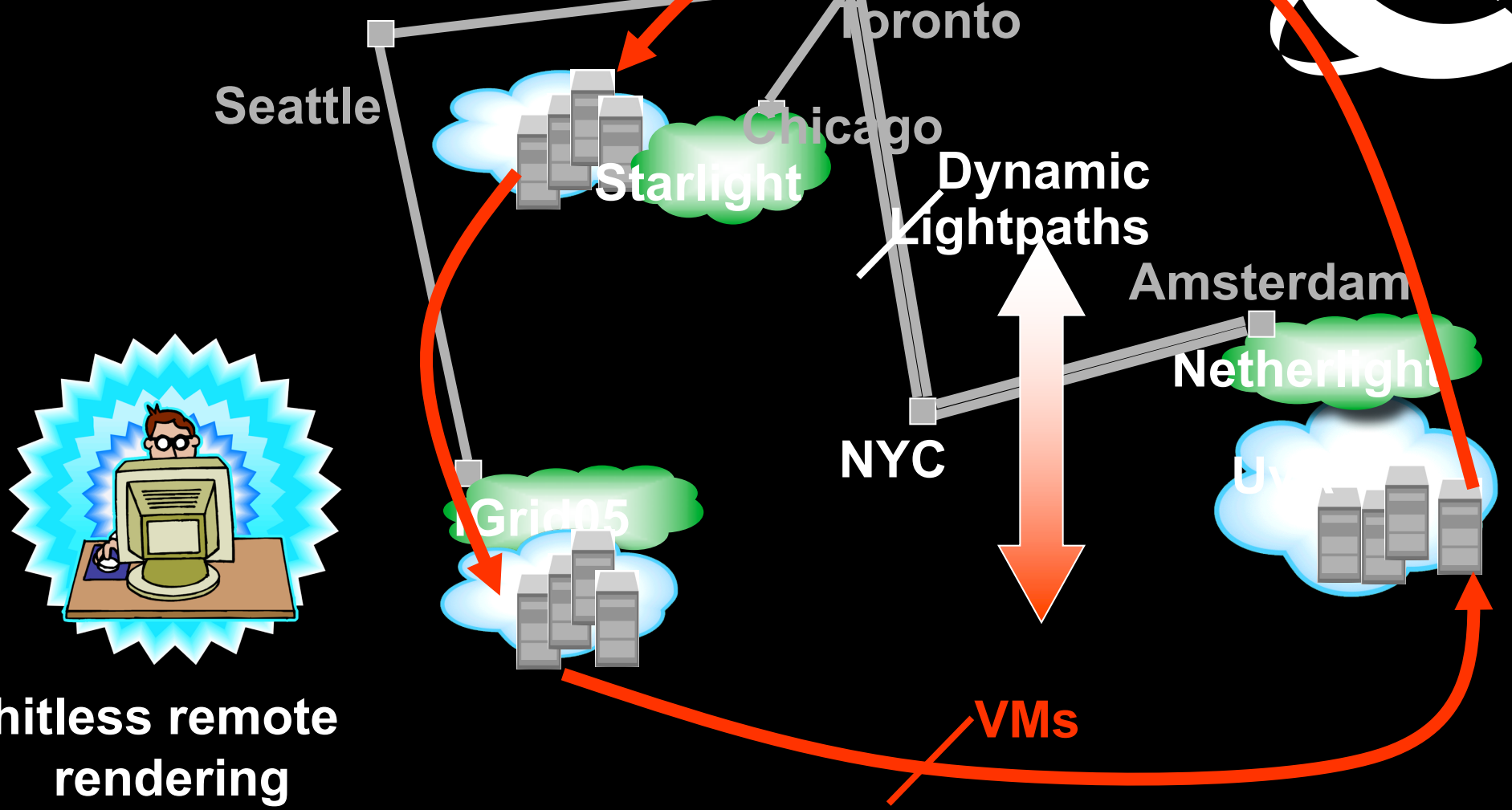
Cybersecurity Big Data
NWO COMMIT/
SARNET project
3.5 FTE



Data Processing models

- Bring data to computing
- Bring computing to data
- Bring computing and data to (un)trusted third party
- A mix of all of the above
- Block chain to record what happened
- Block chain for data integrity
- Bring the owner of Data in control!
- Data owner policy + PEP technology

The VM Turntable Demonstrator



hitless remote rendering

The VMs that are live-migrated run an iterative search-refine-search workflow against data stored in different databases at the various locations. A user in San Diego gets hitless rendering of search progress as VMs spin around

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 \leq 1 sec

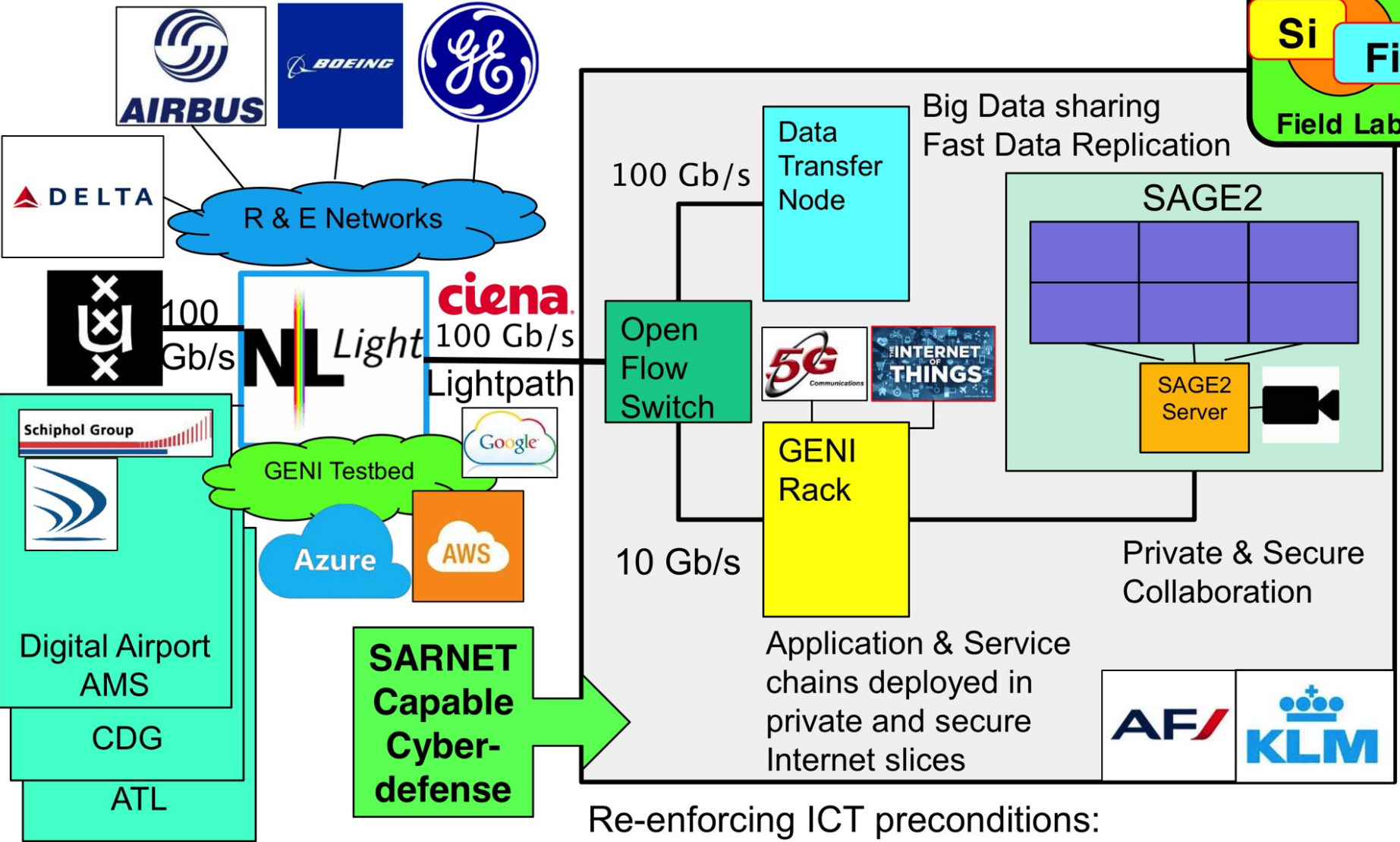
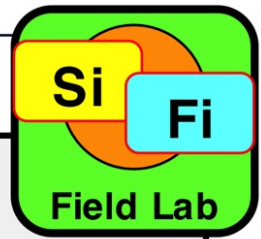
- Back to back, 1GE, RTT = 0.2-0.5 msec, downtime = \sim 0.2 sec*

**Clark et al. NSDI 05 paper. Different workloads*

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

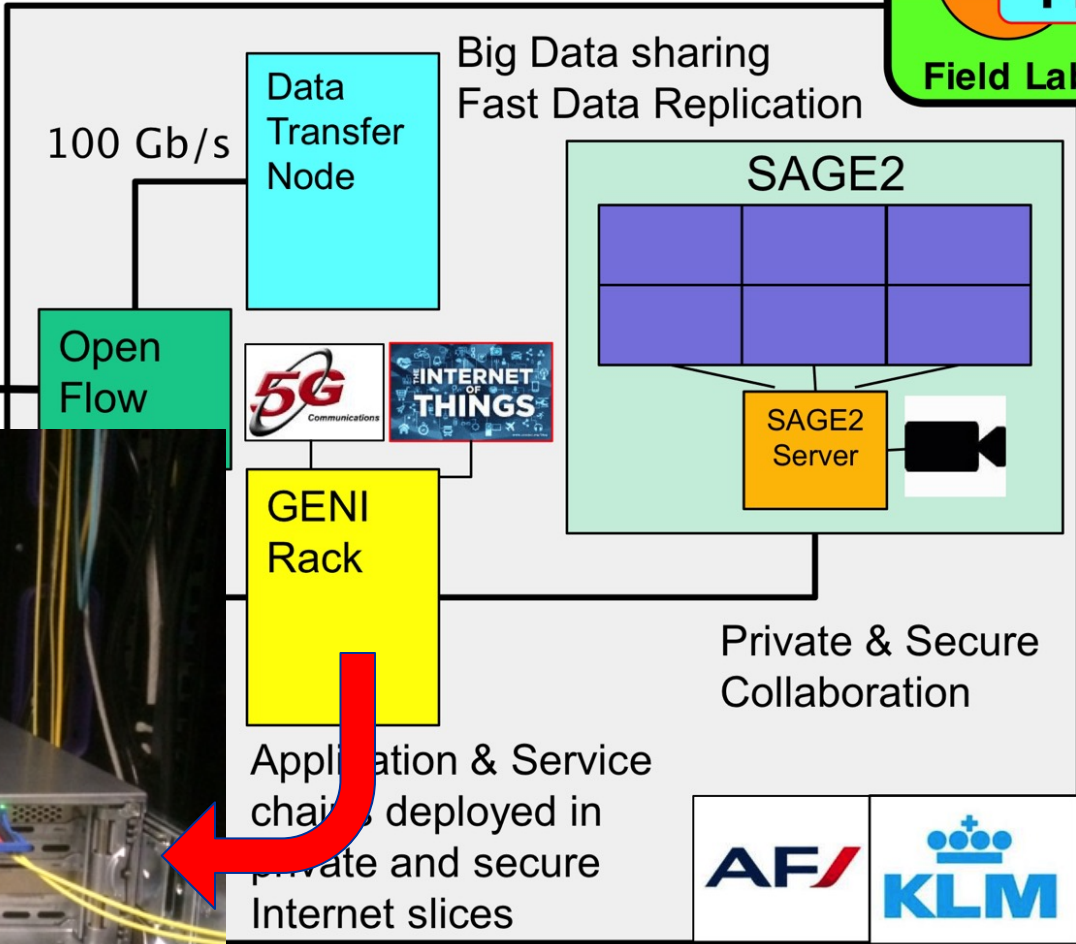
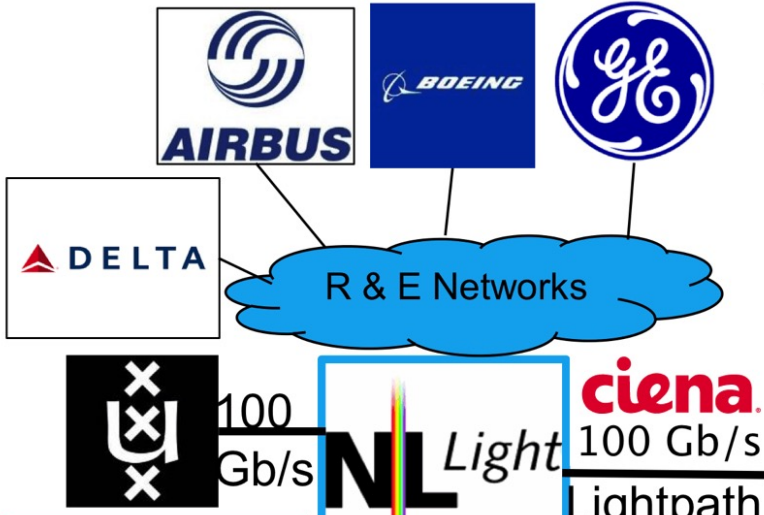
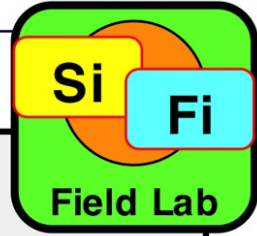
We believe it's a representative instance of active cpu+data+net orchestration

Ambition to put capabilities into fieldlab



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

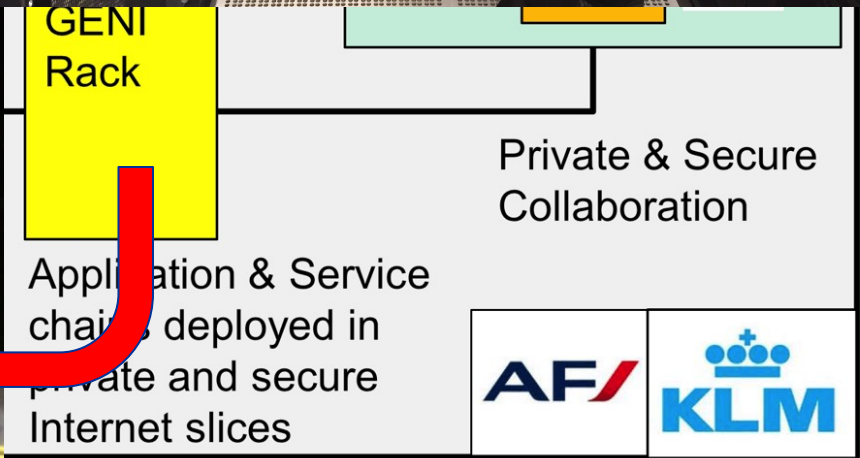
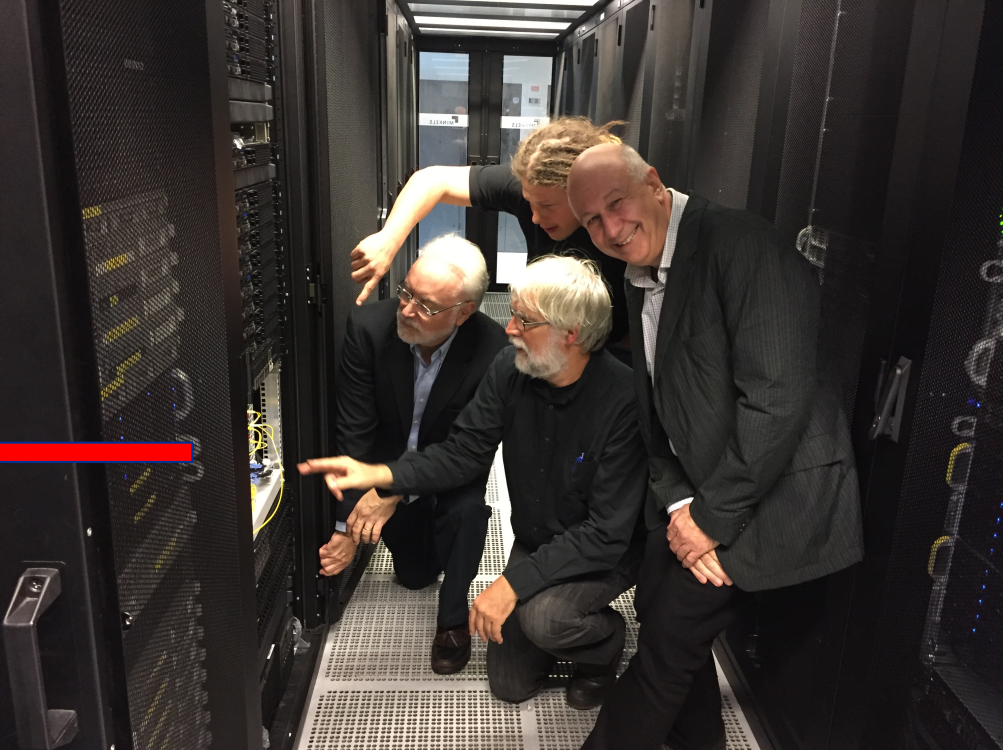
Ambition to put capabilities into fieldlab



ing ICT preconditions:
saged site has similar elements

AF/KLM
FieldLab

Ambition to put o

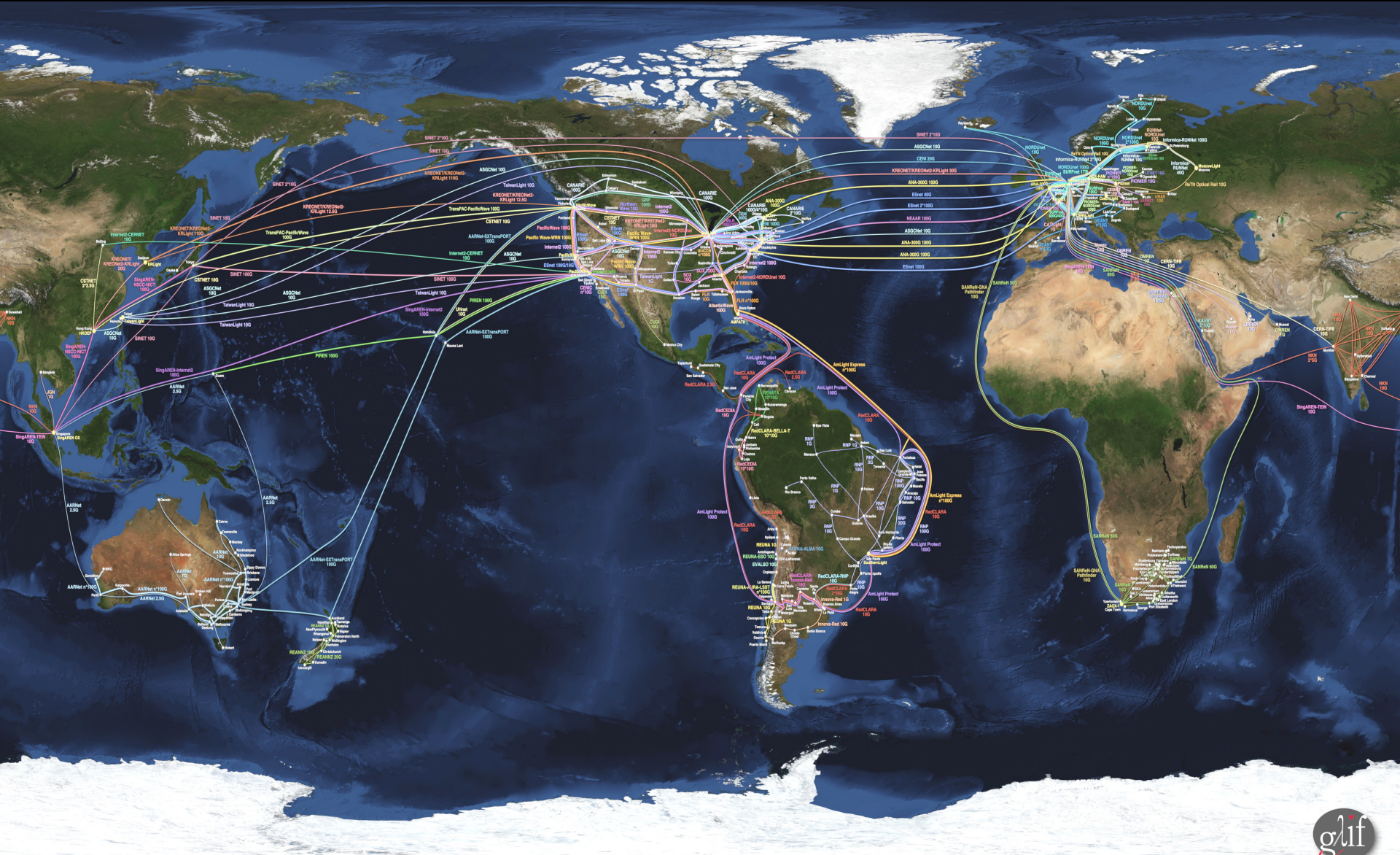


ing ICT preconditions:
saged site has similar elements

AIRFRANCE / KLM

The GLIF – LightPaths around the World

F Dijkstra, J van der Ham, P Grosso, C de Laat, "A path finding implementation for multi-layer networks",
Future Generation Computer Systems 25 (2), 142-146.



SAE Use Case envisaged research collaboration

Funding Agency



Big Data Hub / Spoke or Industry initiative funding



International Networking



Regional / National Networking



Local University



Aircraft MRO, OEM & Operators



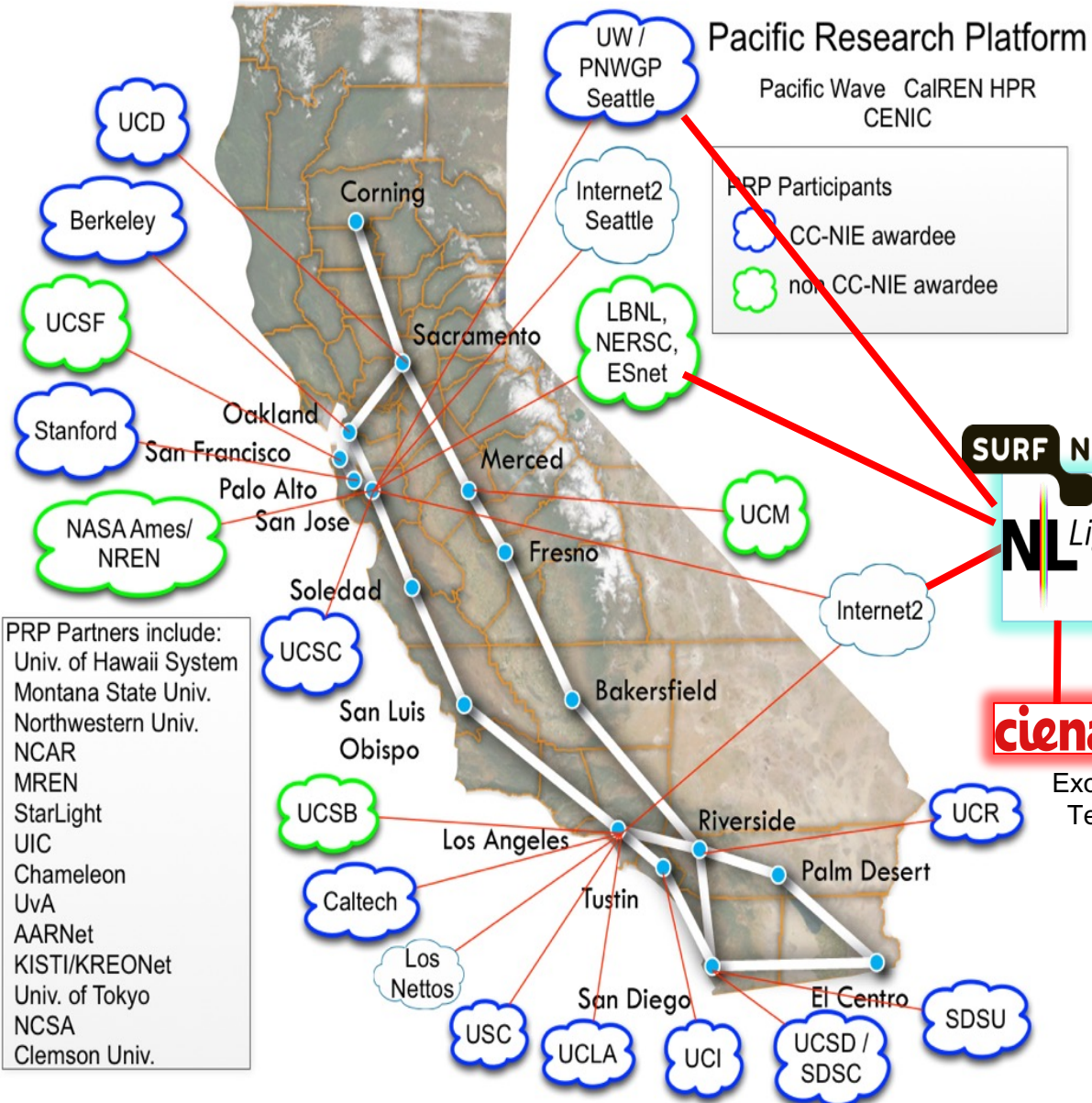
Industry Standards Body



SAE AeroSpace Group
HM-1 working group
Use Case on aircraft sensor Big Data

Pacific Research Platform testbed involvement

Research goal:
Explore value of academic network research capabilities that enable innovative ways & models to share big data assets



ExoGENI Testbed

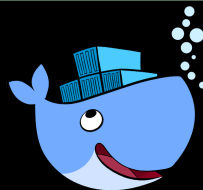


Approach

- Strategic:
 - Translate legislation into machine readable policy
 - Define data use policy
 - Trust evaluation models & metrics
- Tactical:
 - Map app given rules & policy & data and resources
 - Bring computing and data to (un)trusted third party
 - Resilience
- Operational:
 - TPM & Encryption schemes to protect & sign
 - Policy evaluation & docker implementations
 - Use VM and SDI/SDN technology to enforce
 - Block chain to record what happened (after the fact!)



Secure Policy Enforced Data Processing



- Bringing data and processing software from competing organisations together for common goal
- Docker with encryption, policy engine, certs/keys, blockchain and secure networking
- Data Docker (virtual encrypted hard drive)
- Compute Docker (protected application, signed algorithms)
- Visualization Docker (to visualize output)

Org 1

Org 2

Untrusted Unsecure Cloud or SuperCenter

Secure Virtual PC

Data-1

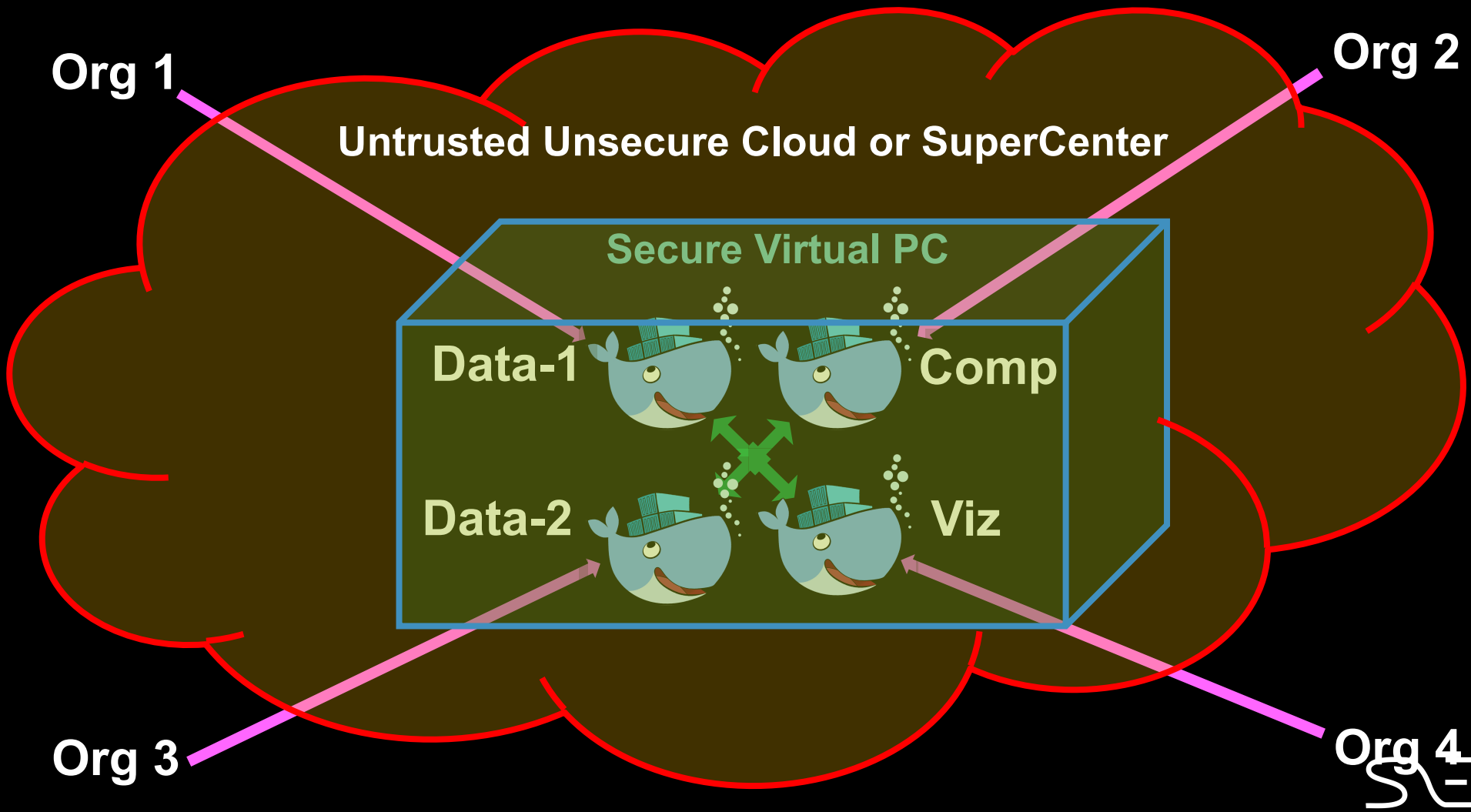
Comp

Data-2

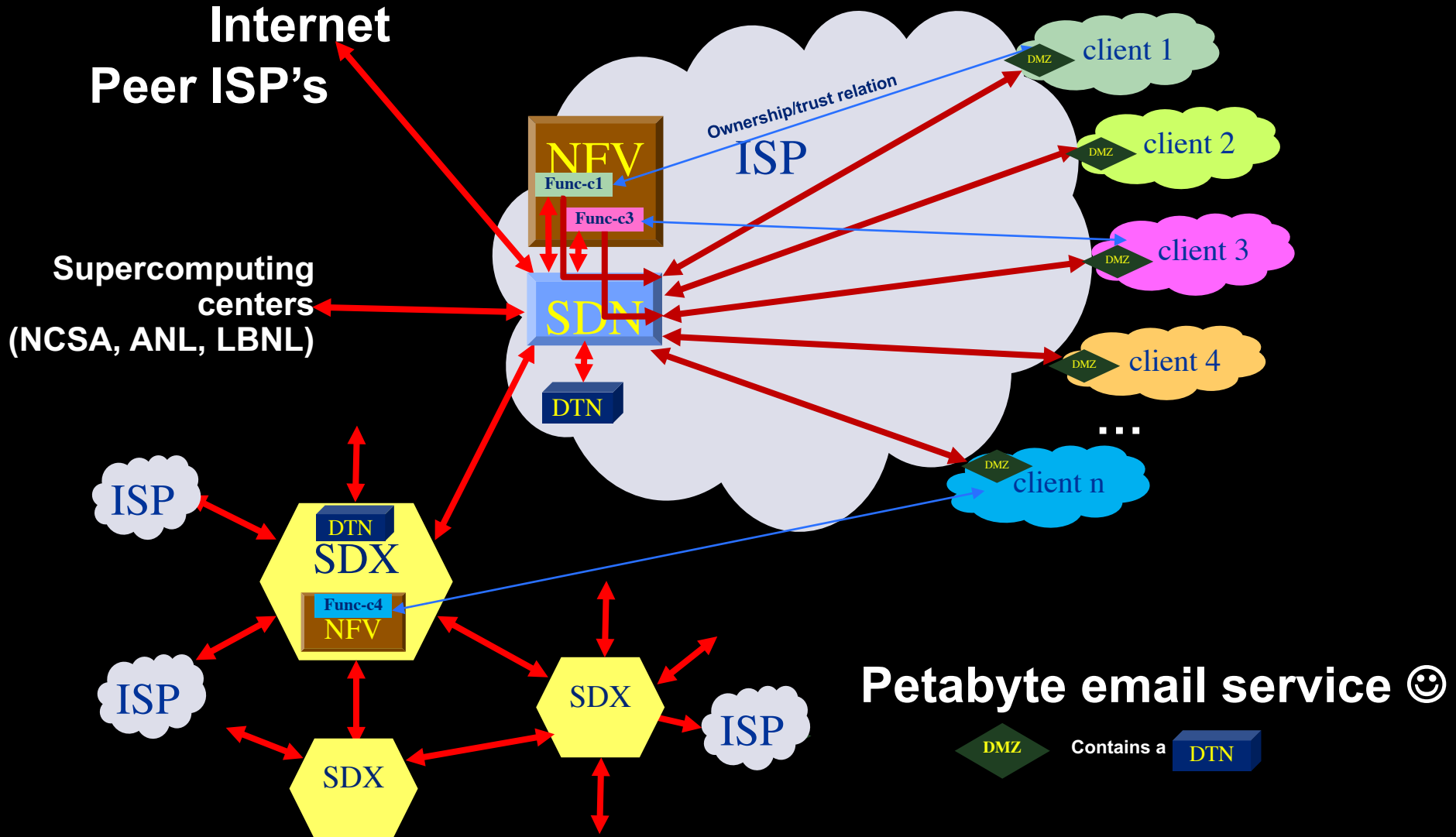
Viz

Org 3

Org 4



Networks of ScienceDMZ's & SDX's



Q&A

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