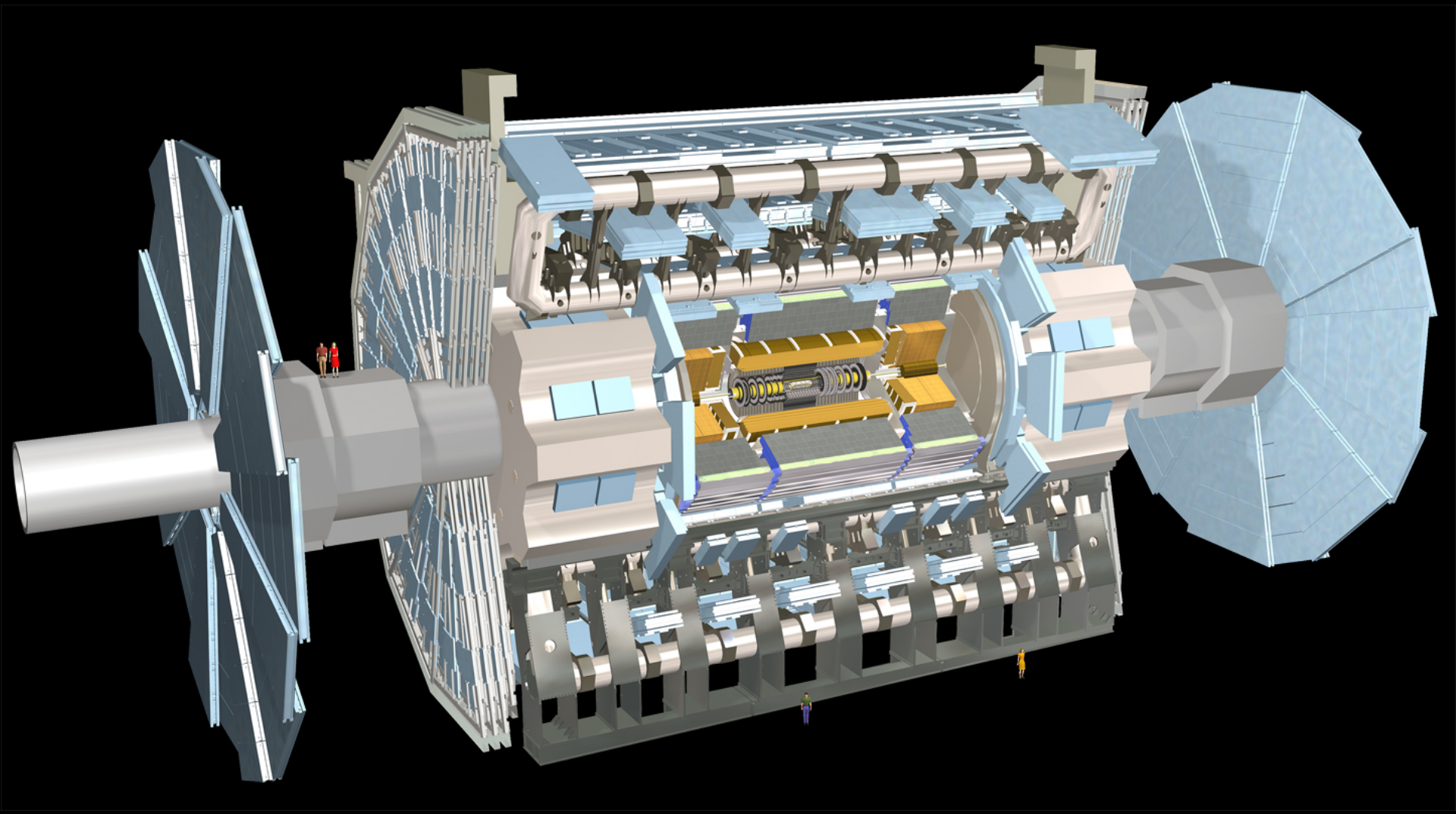
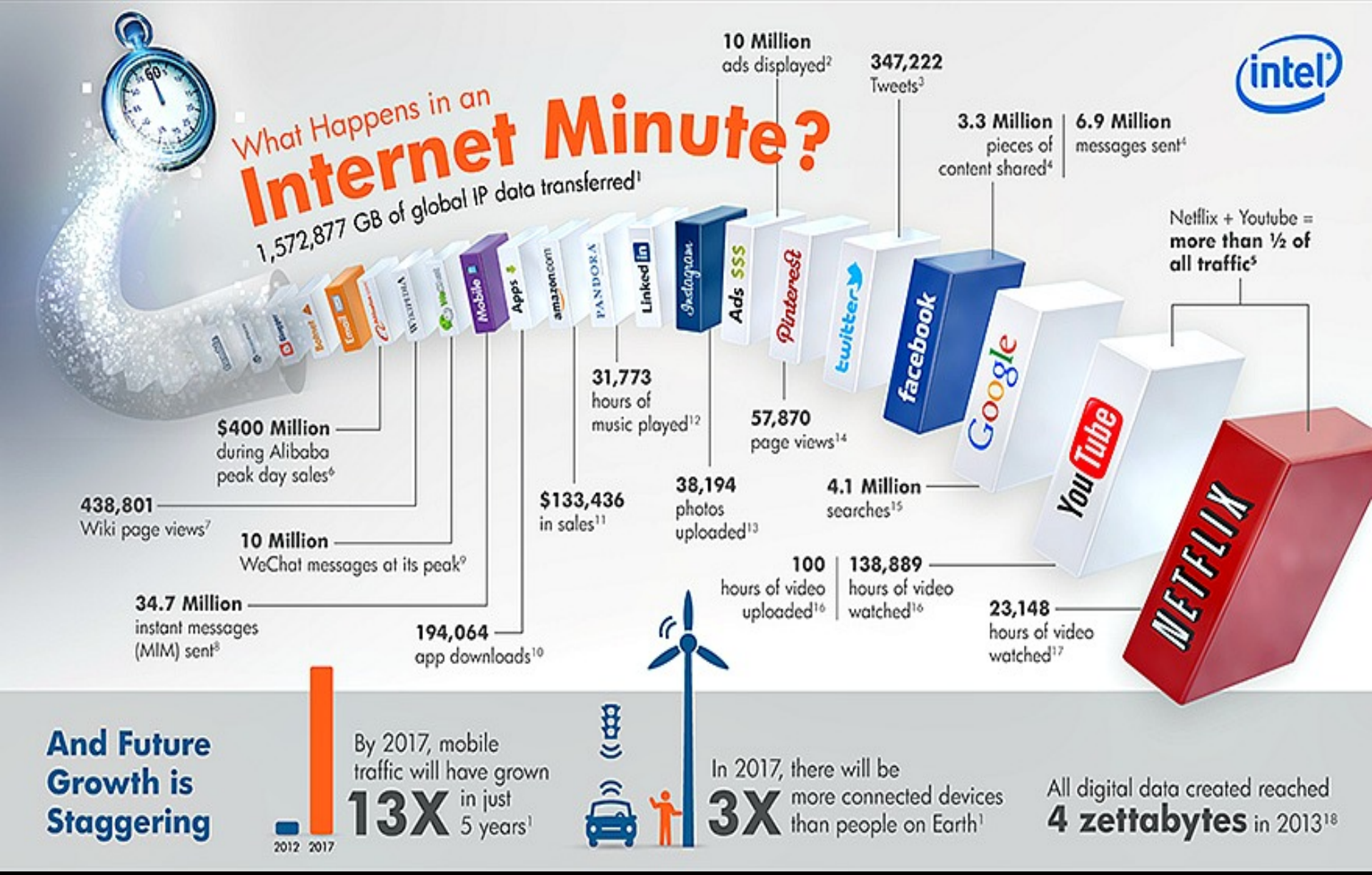
Enabling E-Science Applications with Dynamic Optical Networks: Secure Autonomous Response Networks.

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 (presenter)

System & Network Engineering
University of Amsterdam

ATLAS detector @ CERN Geneve





1,572,877 GByte/minute =
(8*1,572,877*10^9/60 bit/s)/(10*10^12 bit/s per fiber) =
21 fibers with each about 100 * 100 Gb/s channels

Trucks of Tapes

THE WALL STREET JOURNAL.

Amazon Uses Trucks to Drive Data Faster

PERSONAL TECHNOLOGY

The Cable-Cutting Dream Is Kind ...

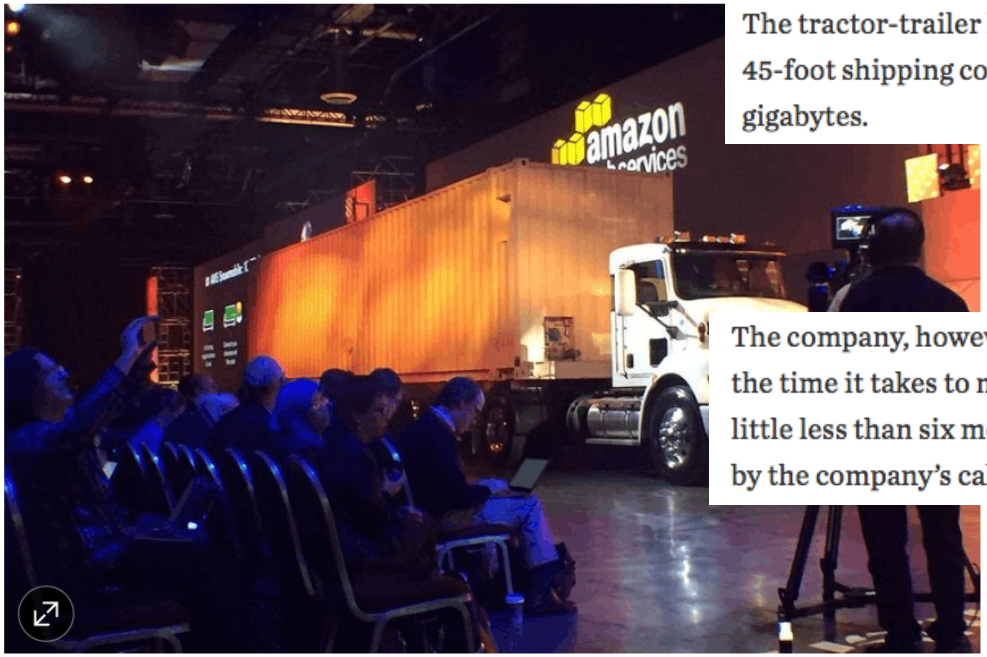
Altice Plans Fiber Upgrade That Could Leave Rivals in the Dust

Netflix Now Lets You Download, But Many Top Shows Are Off Limits

TECH

Amazon Uses Trucks to Drive Data Faster

Cloud-computing unit, Amazon Web Services, unveils new offerings at annual conference in Las Vegas



Amazon unveiled the 'Snowmobile' service on Wednesday in Las Vegas. *PHOTO: AMAZON WEB SERVICES*

The tractor-trailer hauls a massive storage device, dubbed Snowmobile, in the form of a 45-foot shipping container that holds 100 petabytes of data. A petabyte is about 1 million gigabytes.

The company, however, isn't promising lightning speed. Ten Snowmobiles would reduce the time it takes to move an exabyte from on-premises storage to Amazon's cloud to a little less than six months, from about 26 years using a high-speed internet connection, by the company's calculations.

By JAY GREENE By LAURA STEVENS

Updated Nov. 30, 2016 7:19 p.m. ET

4 COMMENTS

LAS VEGAS—In Amazon Web Services, Amazon.com Inc. has built one of the most powerful computing networks in the world, on pace to post more than $12 billion in revenue this year.

But the retail giant on Wednesday proposed a surprising way to move data from large corporate customers' data centers to its public cloud-computing operation: by truck.

Networks can move massive amounts of data only so fast. Trucks, it turns out, can move it faster.

Most Popular

1. U.S. to Fo… Least $10… Student … Coming …
2. Opinion: Trump's … Pick Sca…
3. Trump's … His Busi… Draws Q…
4. Creator … Mac Dies
5. Trump's … Choice S… Absolute…

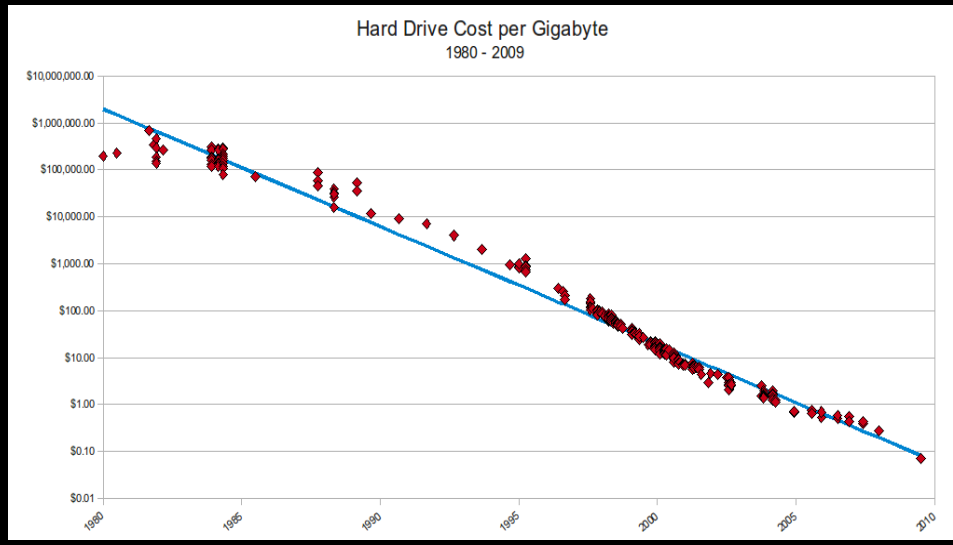
1 fiber does about 16 Tbit/s
= 2 Tbyte/s
⇒ 500000 s/ExaByte
⇒ One week/ExaByte

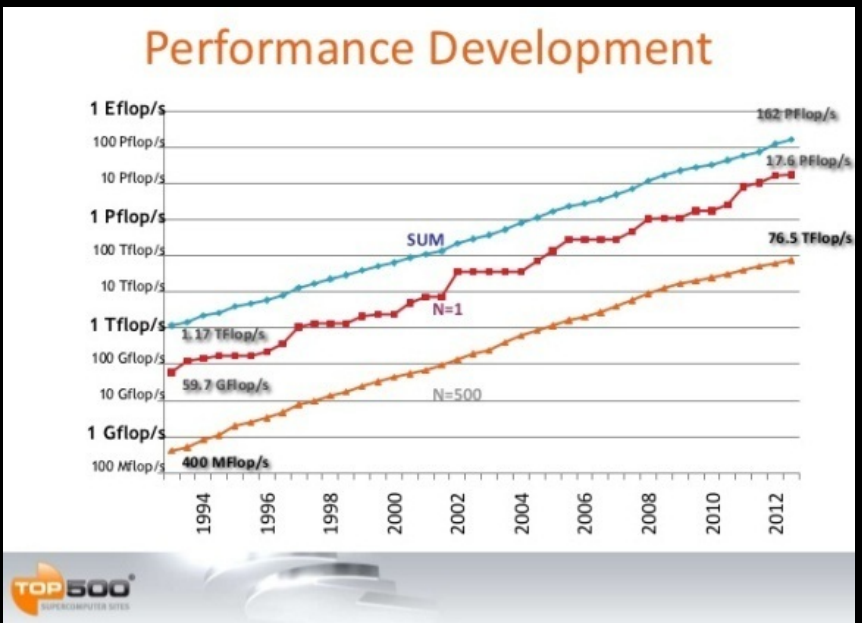
Moore's and Kryders Law

This omnipresence of IT makes us not only strong but also vulnerable.

- A virus, a hacker, or a system failure can instantly send digital shockwaves around the world.

The hardware and software that allow all our systems to operate is becoming bigger and more complex all the time, and the capacity of networks and data storage is increasing by leaps and bounds.



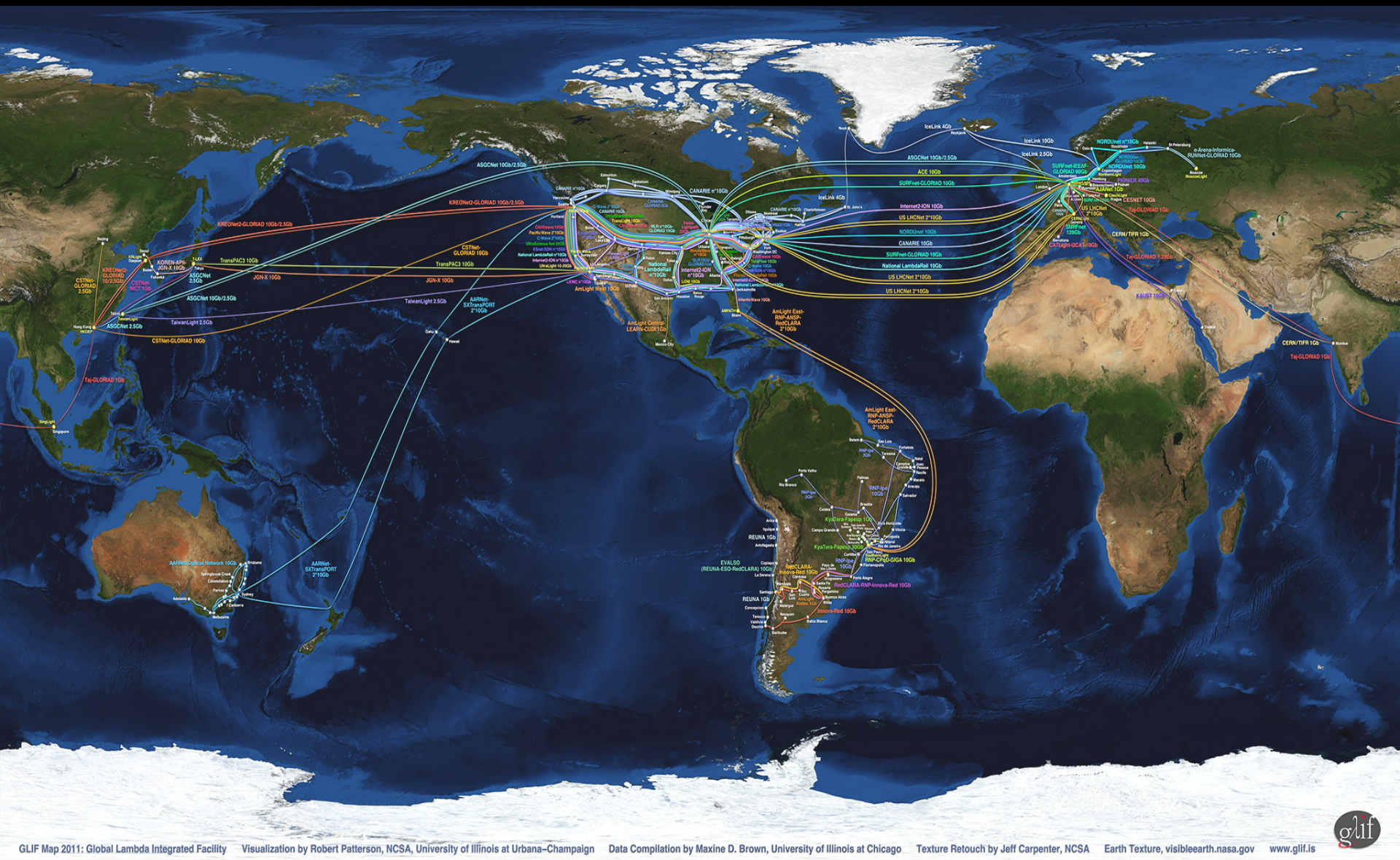


We will soon reach the limits of what is currently feasible and controllable.

http://www.knaw.nl/Content/Internet_KNAW/publicaties/pdf/20111029.pdf

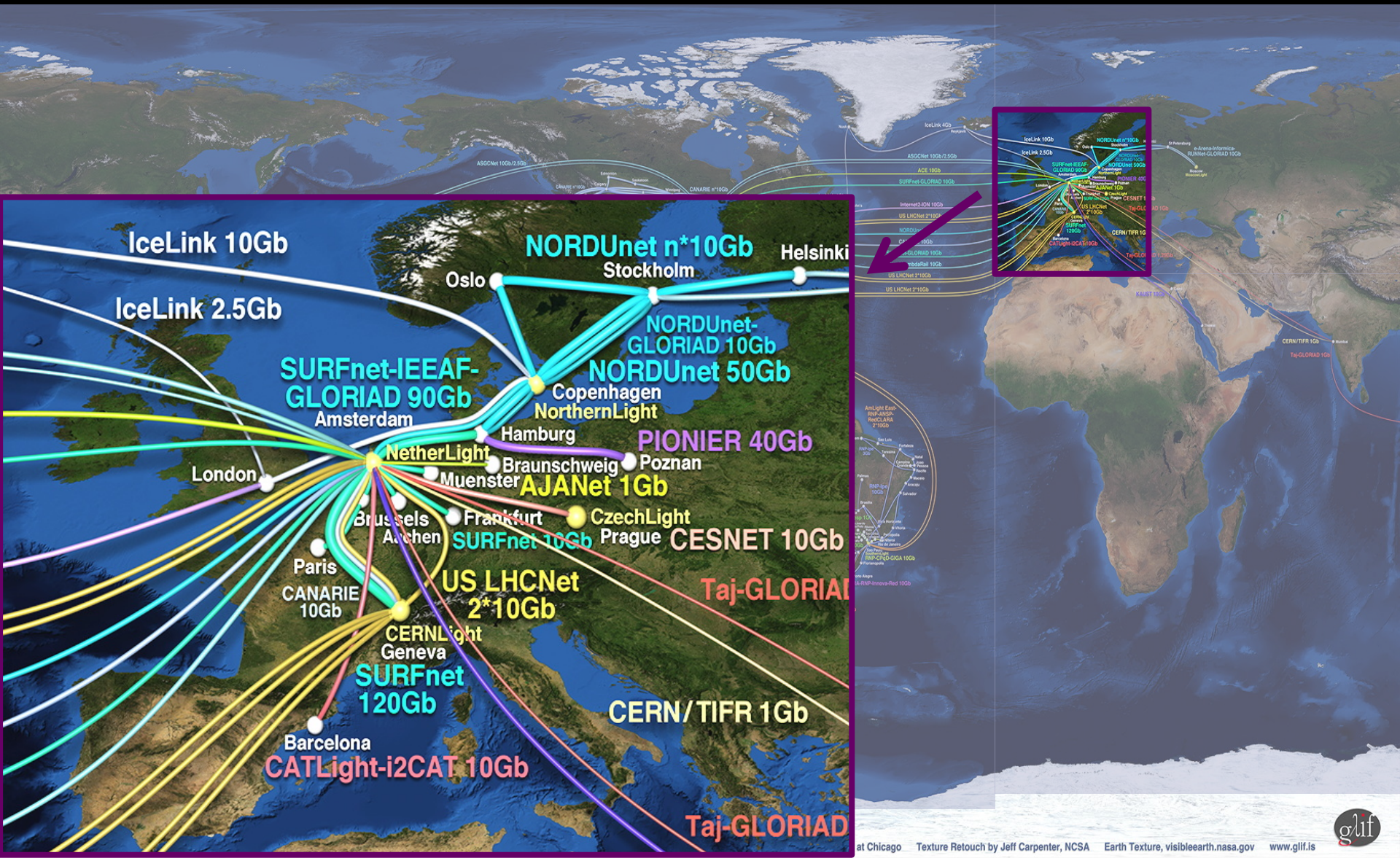
The GLIF – LightPaths around the World

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.



The GLIF – LightPaths around the World

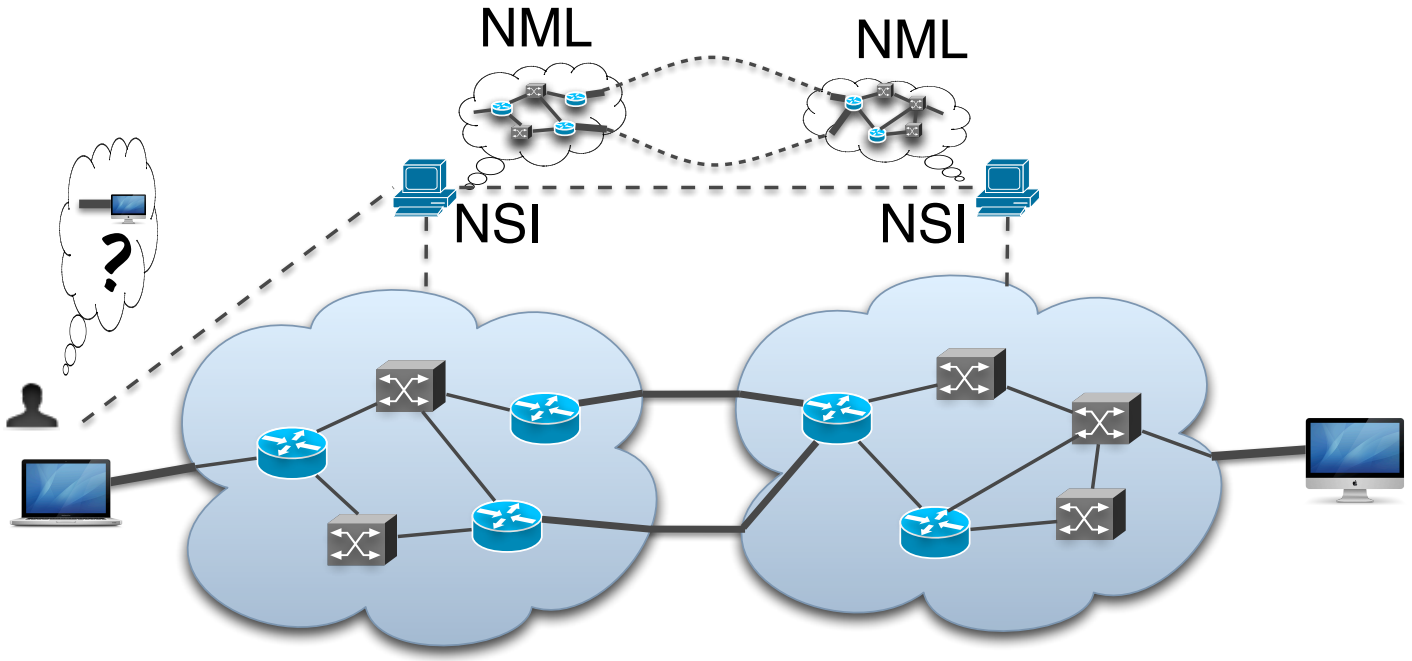
F Dijkstra, J van der Ham, P Grosso, C de Laat, “A path finding implementation for multi-layer networks”, Future Generation Computer Systems 25 (2), 142-146.



Network Topology Description

Network topology research supporting automatic network provisioning

- Inter-domain networks
- Multiple technologies
- Based on incomplete information
- Possibly linked to other resources



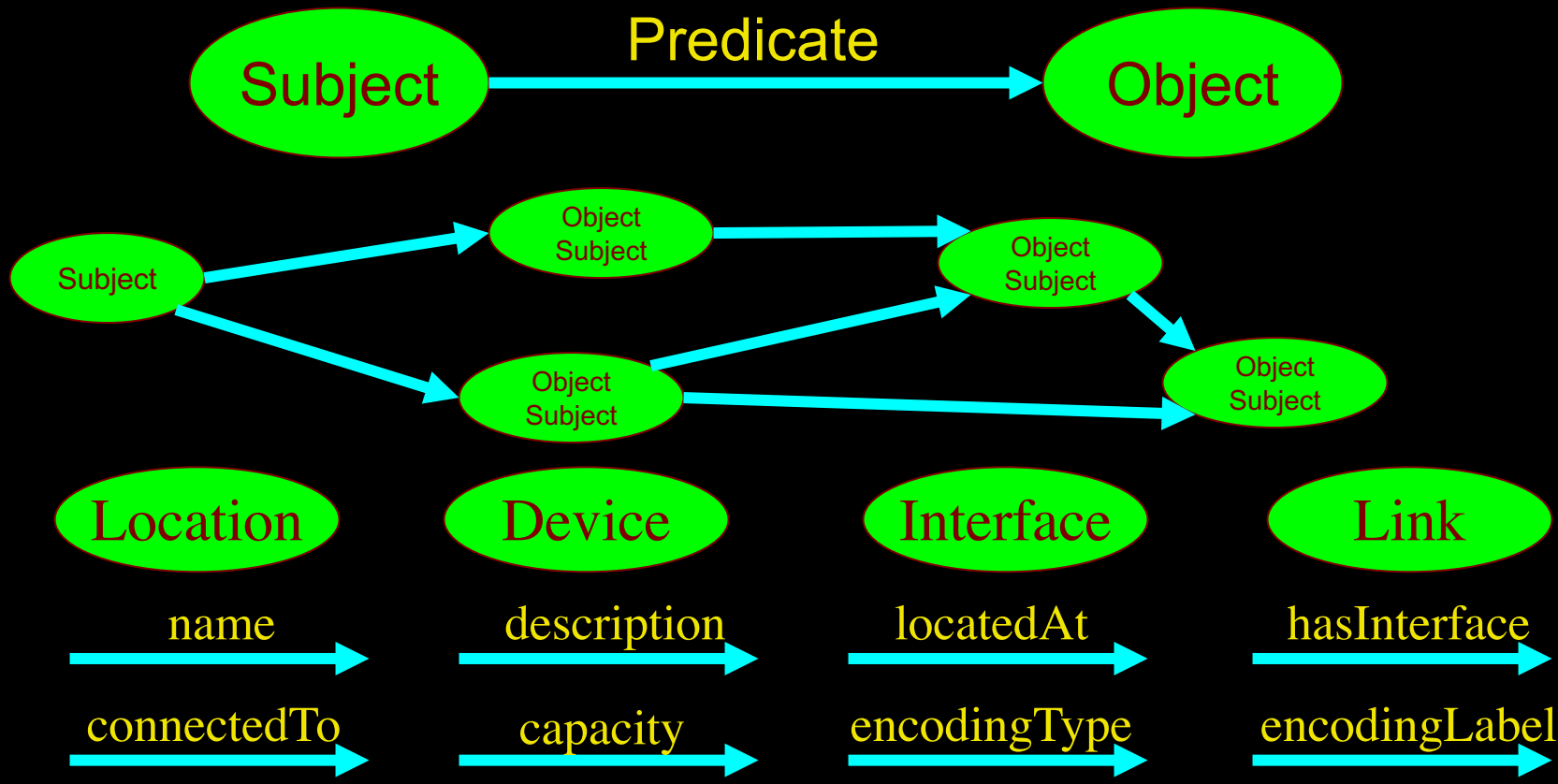
OpenGridForum
OPEN FORUM | OPEN STANDARDS

http://redmine.ogf.org/projects/nml-wg
http://redmine.ogf.org/projects/nsi-wg

http://sne.science.uva.nl/ndl

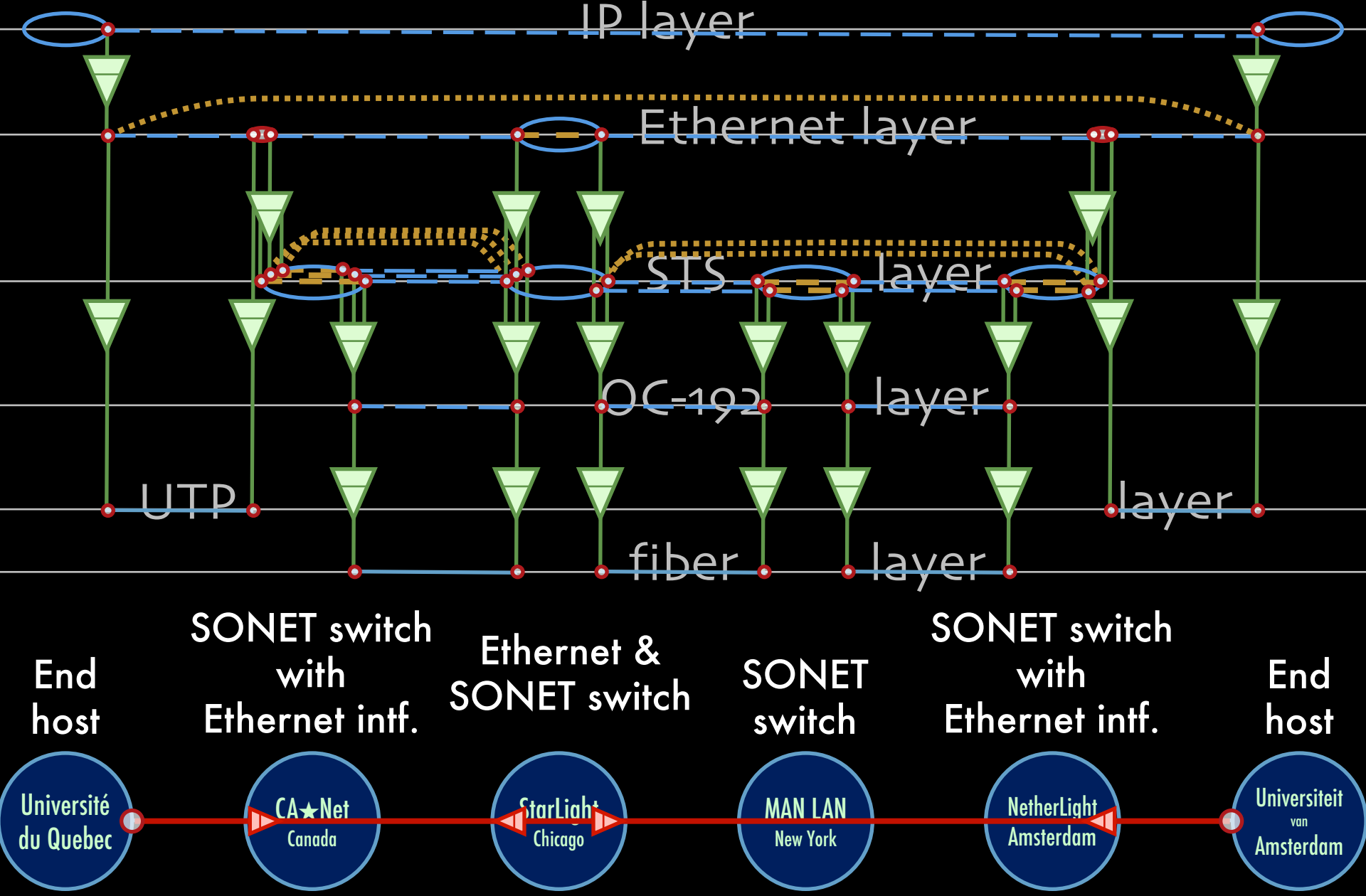
LinkedIN for Infrastructure - iNDL

- From semantic Web / Resource Description Framework.
- The RDF uses XML as an interchange syntax.
- Data is described by triplets (Friend of a Friend):

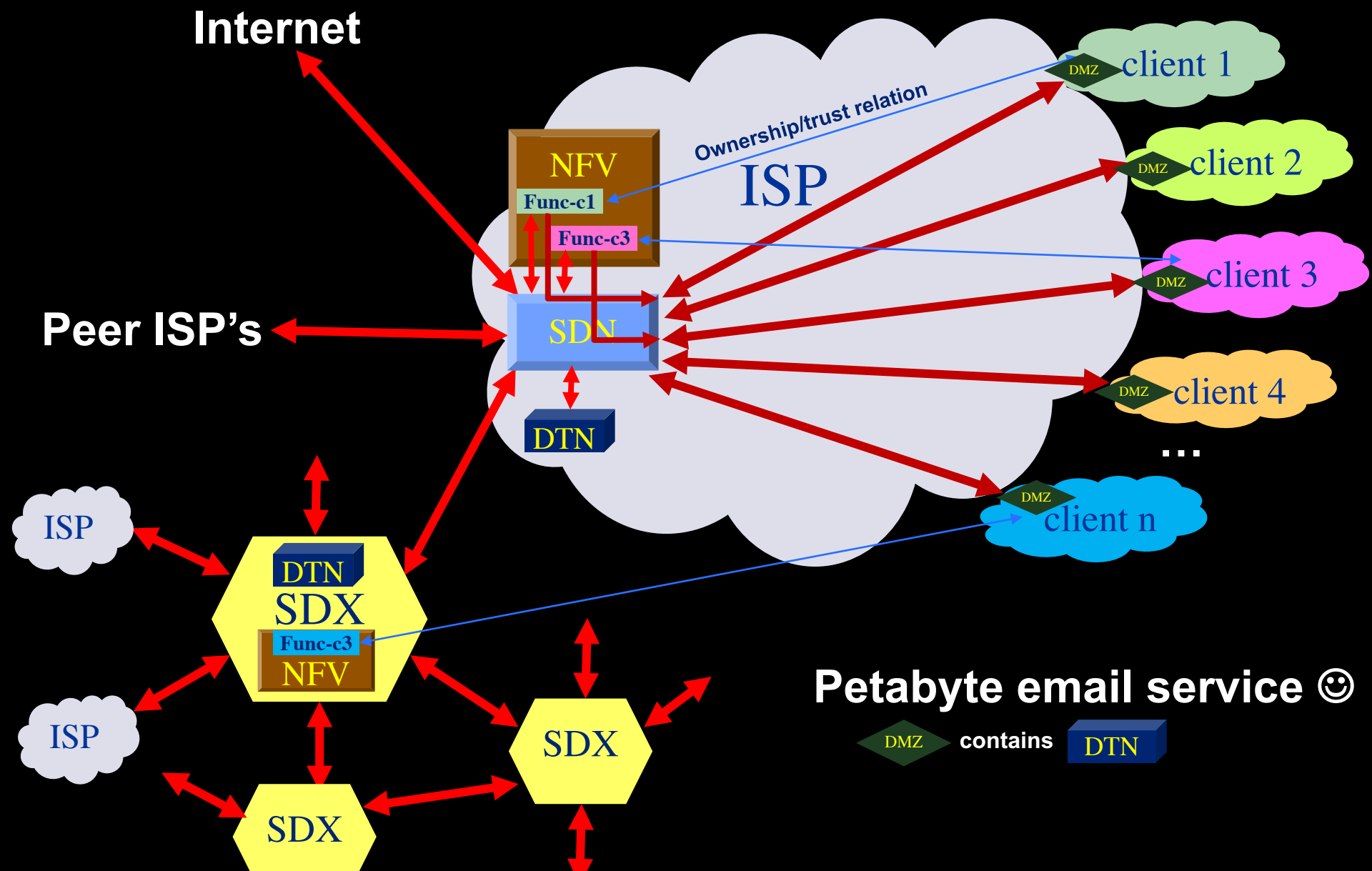


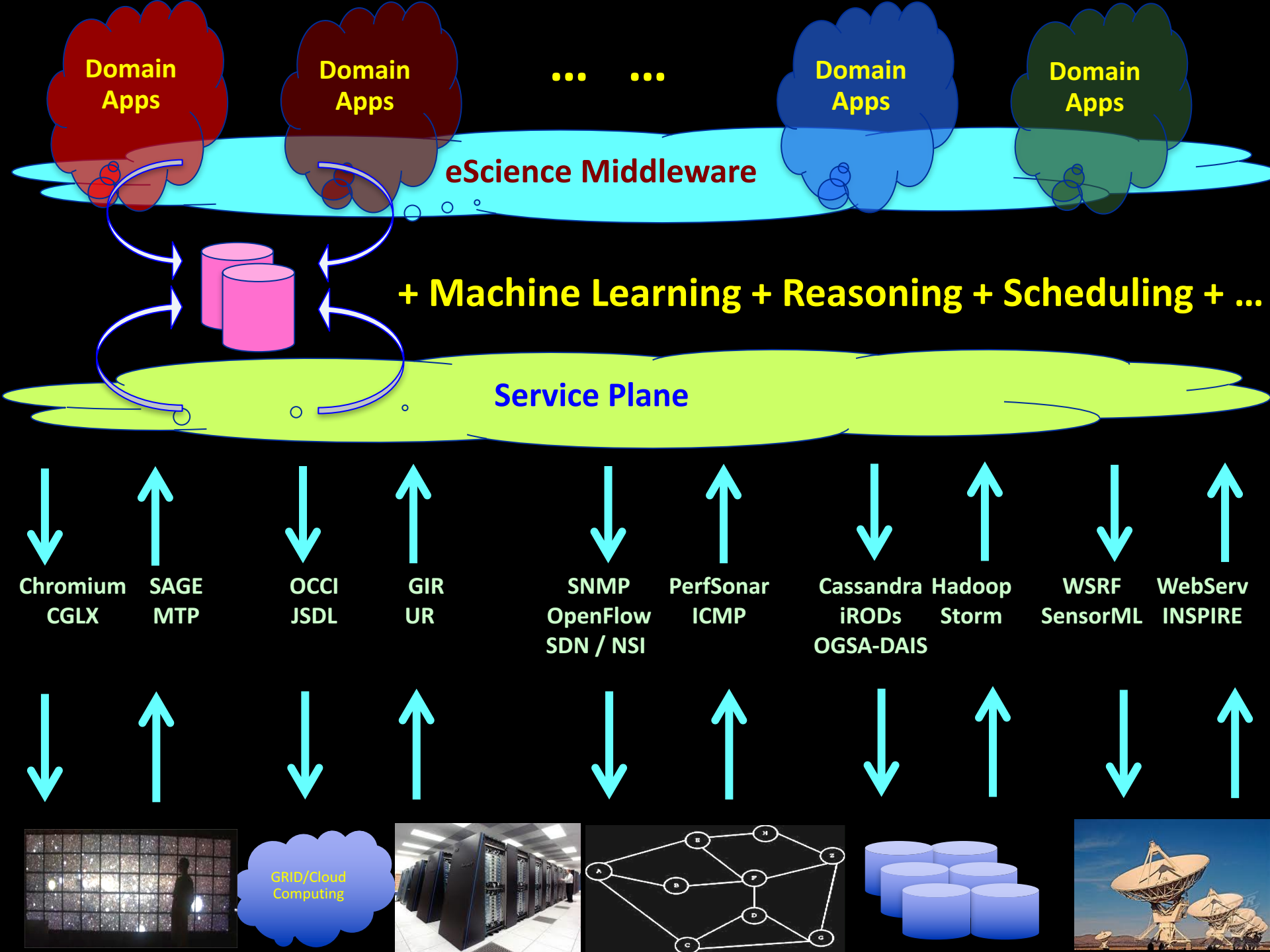
M Ghijsen, J van der Ham, P Grosso, C Dumitru, H Zhu, Z Zhao, C de Laat, "A Semantic-Web Approach for Modeling Computing Infrastructures", Journal of Computers and Electrical Engineering, Elsevier, Volume 39, Issue 8, November 2013, Pages 2553-2565.

Multi-layer descriptions in NDL

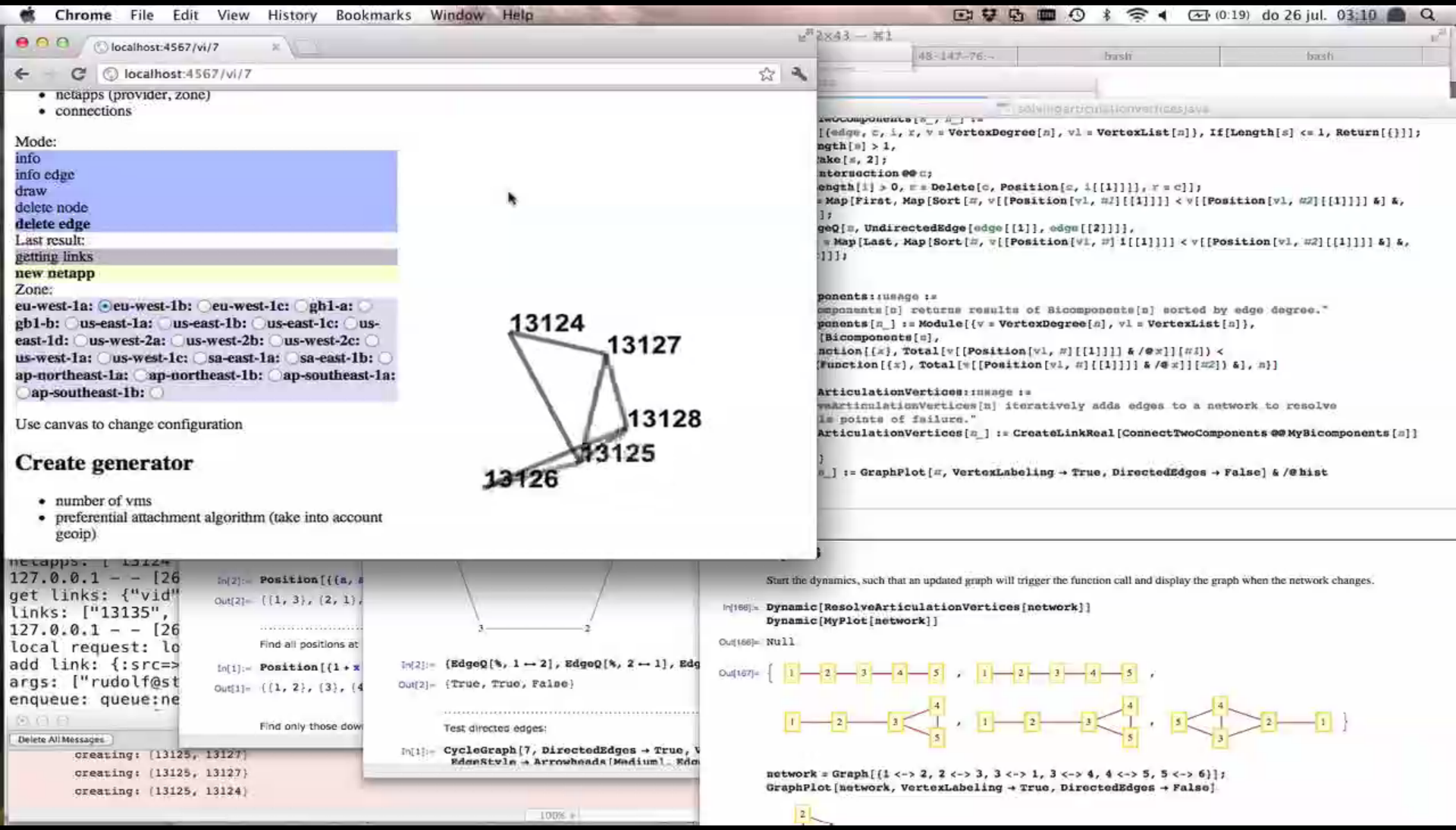


Networks of ScienceDMZ's & SDX's

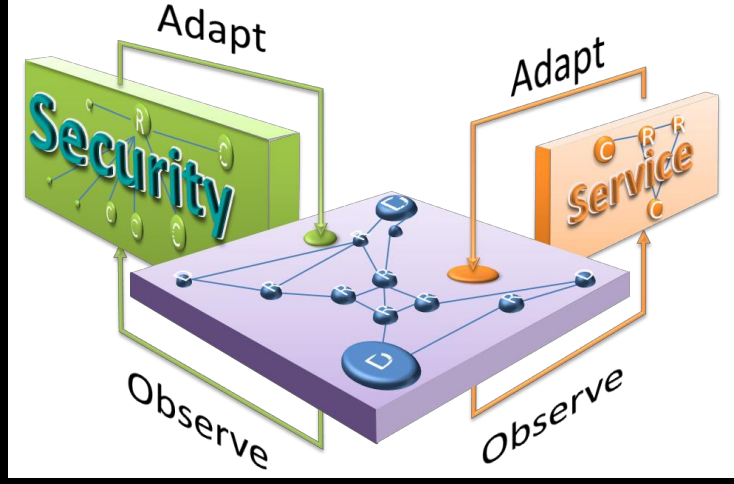



Domain Apps
Domain Apps
... ...
Domain Apps
Domain Apps
eScience Middleware
+ Machine Learning + Reasoning + Scheduling + …
Service Plane
Chromium CGLX
SAGE MTP
OCCI JSDL
GIR UR
SNMP OpenFlow SDN / NSI
PerfSonar ICMP
Cassandra iRODs OGSA-DAIS
Hadoop Storm
WSRF SensorML
WebServ INSPIRE
GRID/Cloud Computing

Basic operating system loop



Cyber security program SARNET



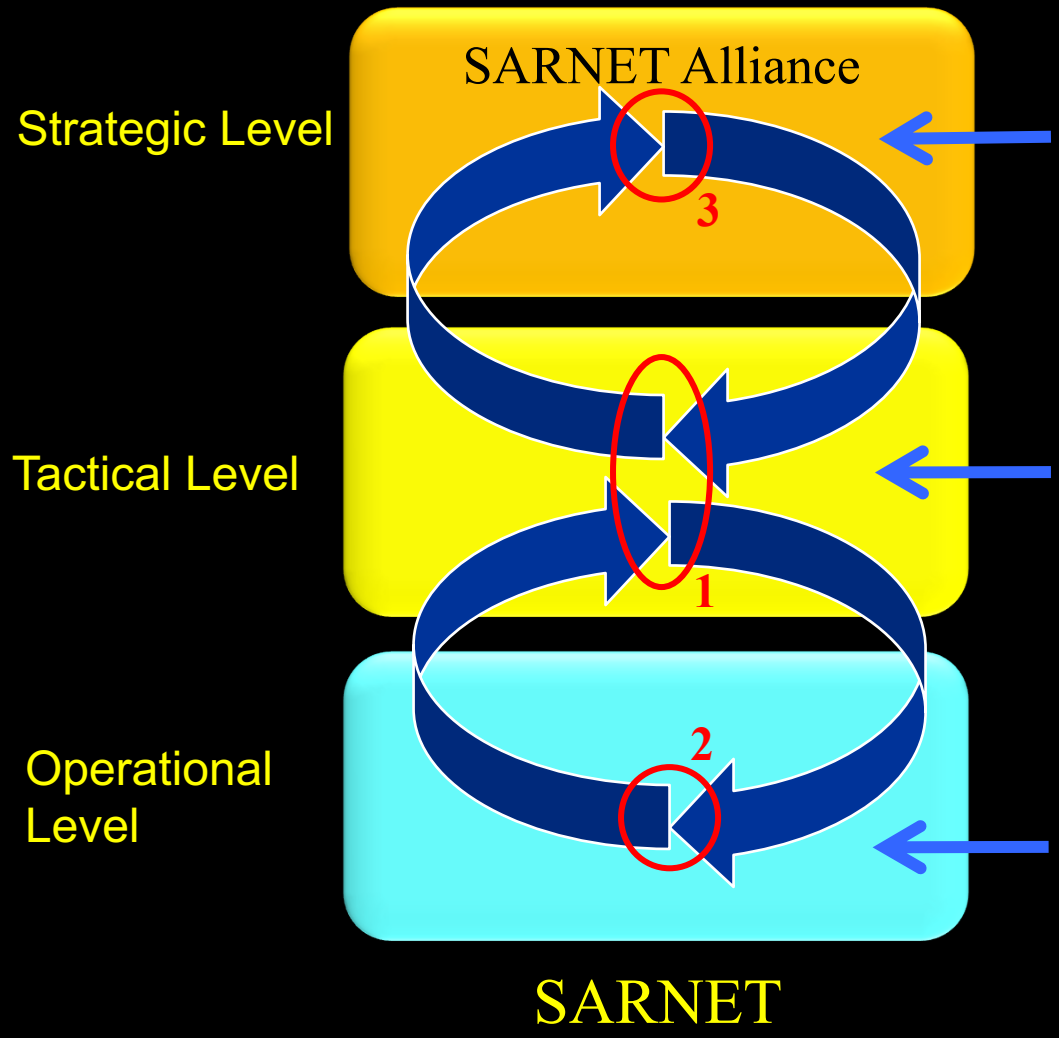
Research goal is to obtain the knowledge to create ICT systems that:

- 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

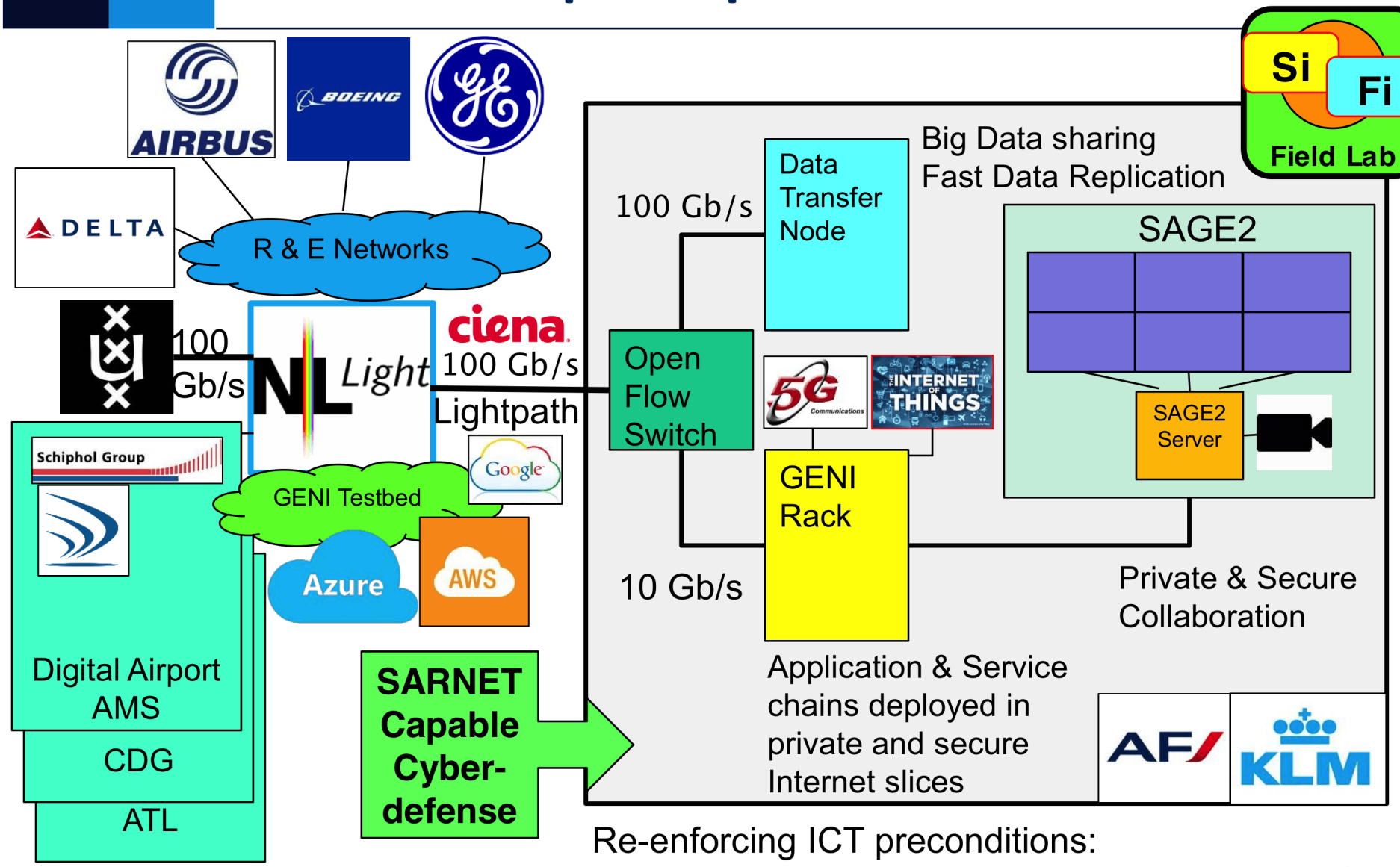


Ameneh Deljoo (PhD):
Why create SARNET Alliances?
Model (3) autonomous SARNET behaviors to identify risk and benefits for SARNET stakeholders

Gleb Polevoy (PD):
Determine best defense scenario against cyberattacks deploying SARNET functions (1) based on security state and KPI information (2).

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).

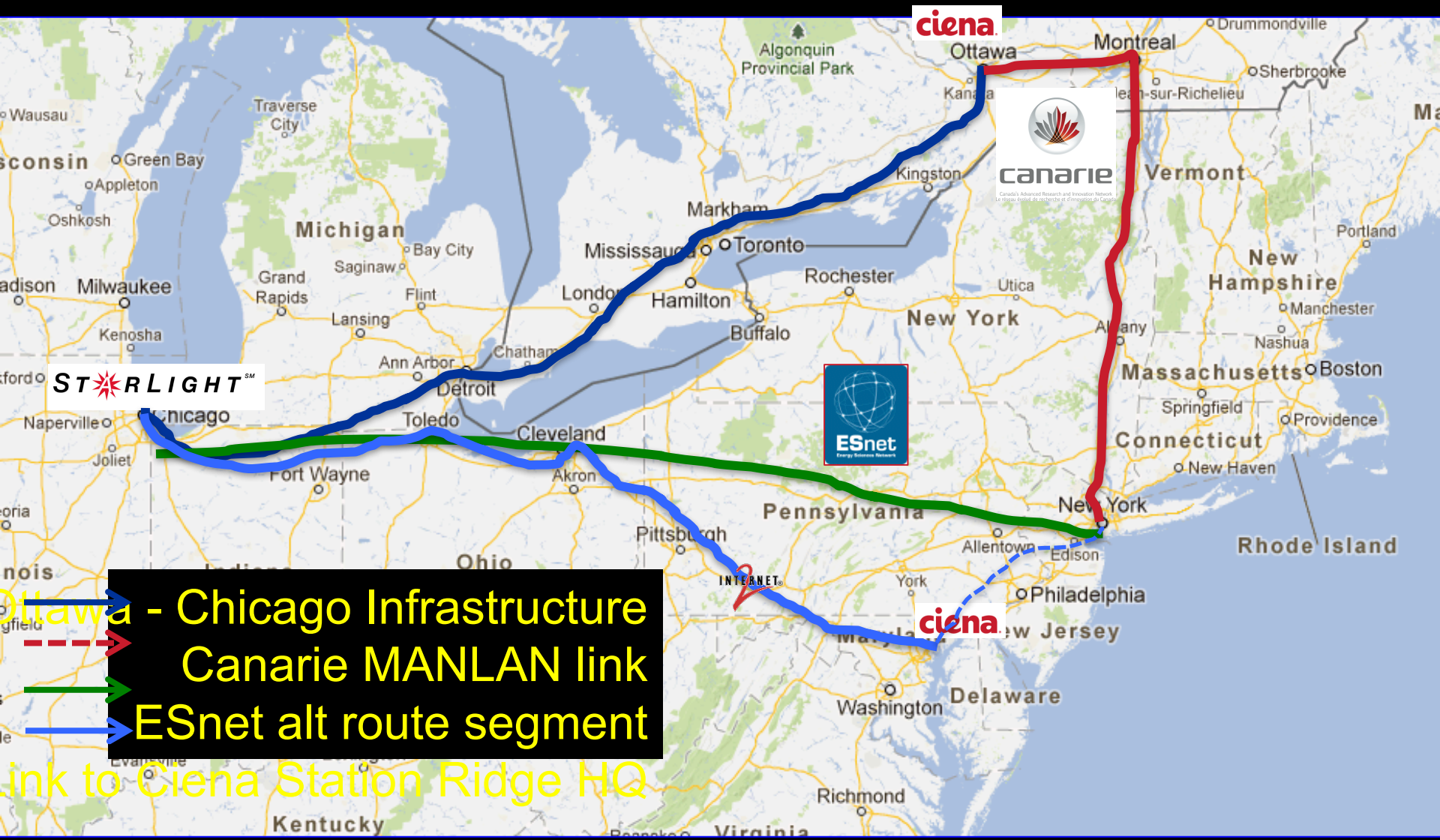
Ambition to put capabilities into fieldlab



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

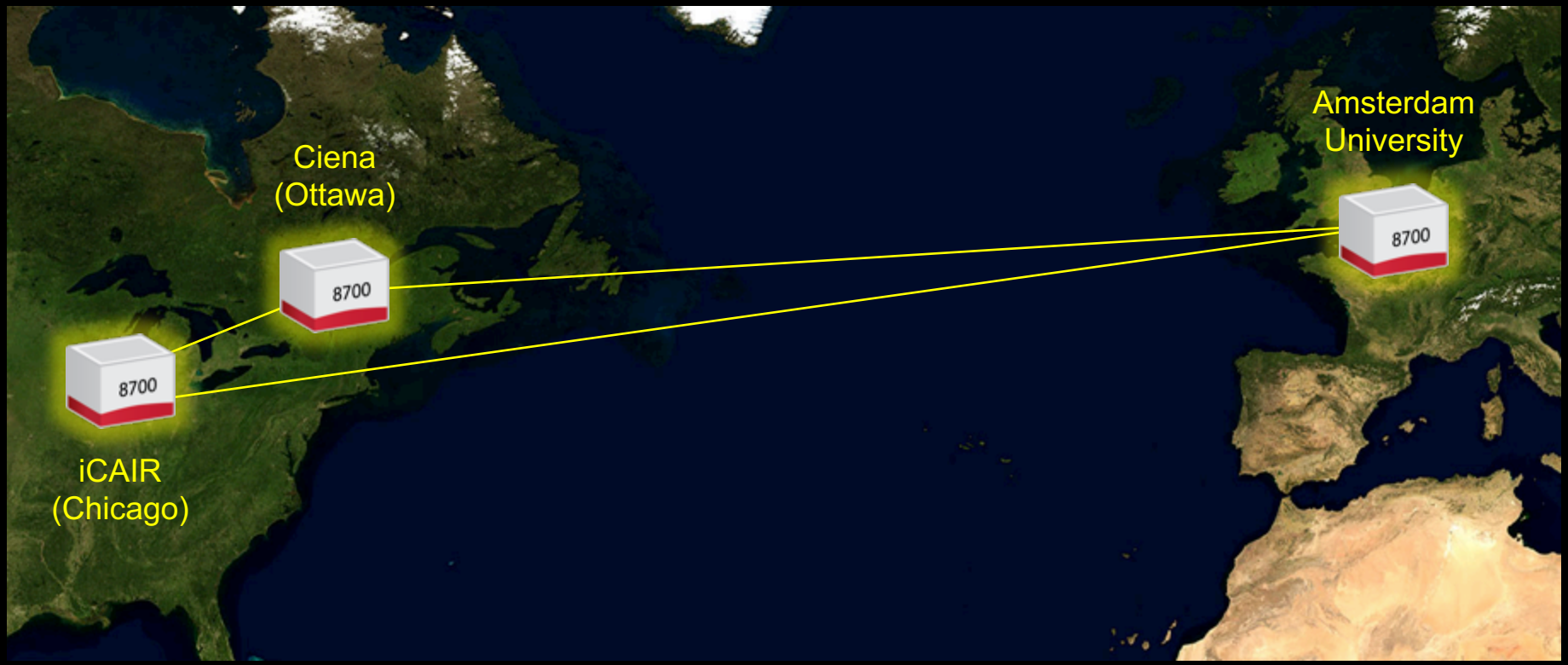
AIRFRANCE KLM

Ciena's CENI topology



CENI, International extension to University of Amsterdam

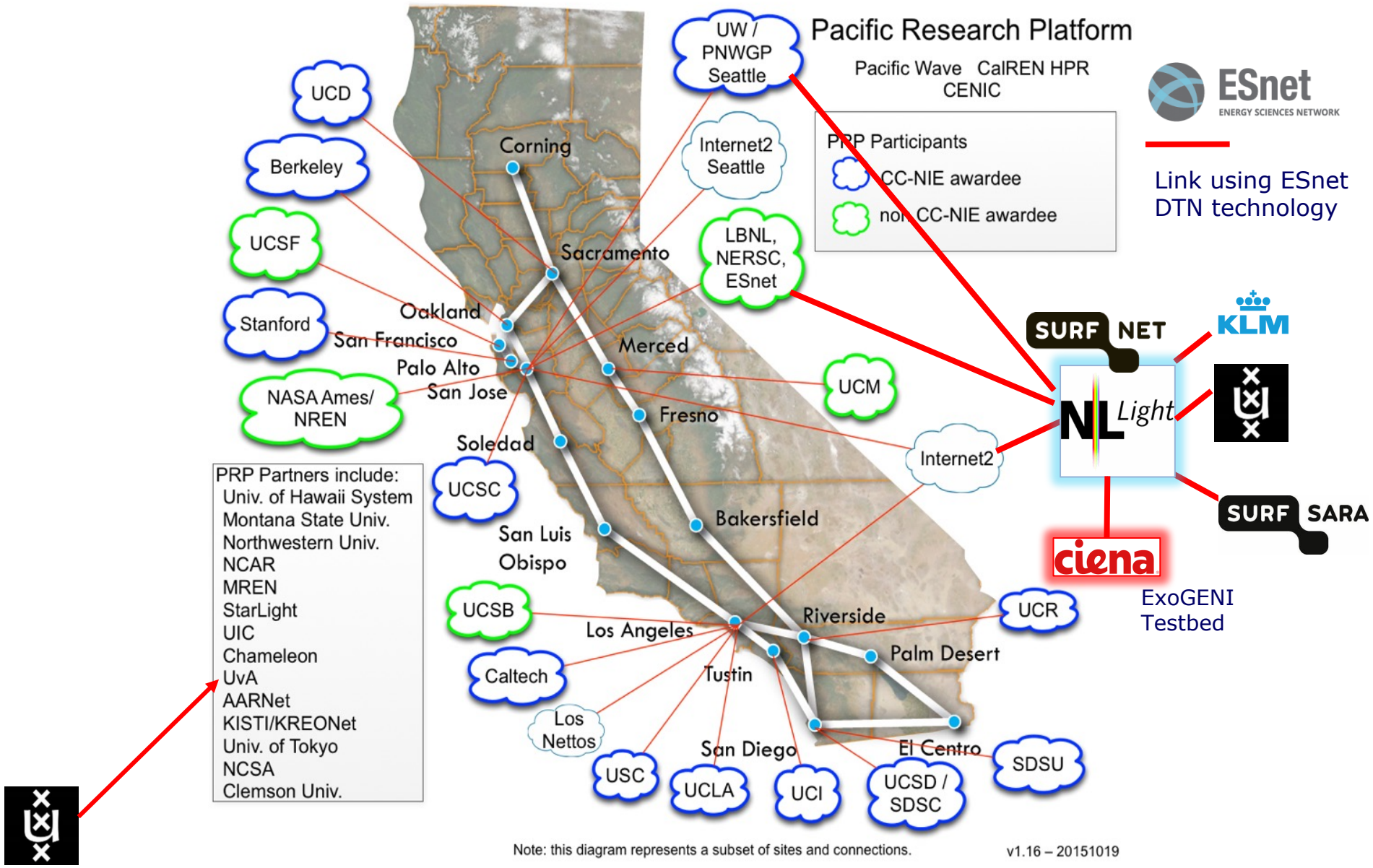
Research Triangle Project. Operation Spring of 2015



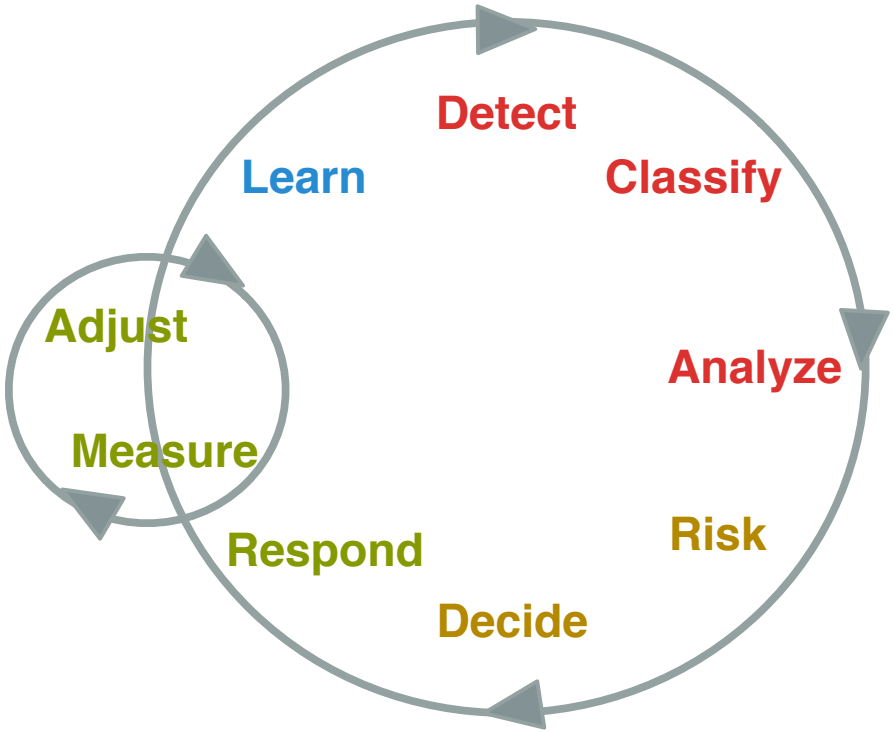
National Science Foundations ExoGENI racks, installed at UvA (Amsterdam), Northwestern University (Chicago) and Ciena's labs (Ottawa), are connected via a high performance 100G research network and trans-Atlantic network facilities using the Ciena 8700 Packetwave platform. This equipment configuration is used to create a computational and storage test bed used in collaborative demonstrations.

ciena

Participation in Pacific Research Platform



Control loop



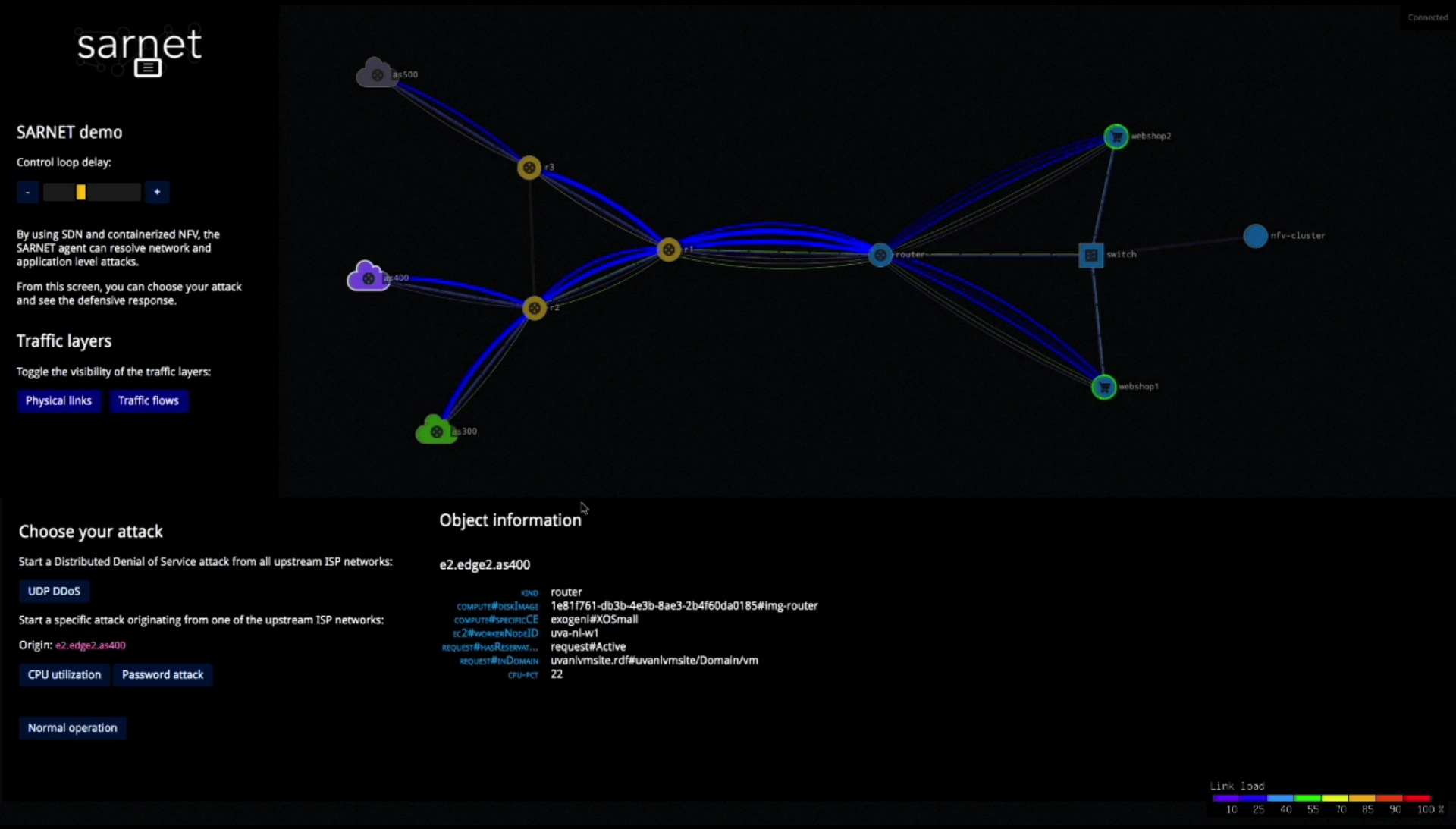
Detection phase: Detect, Classify, Analyze

Decision phase: Risk, Decide

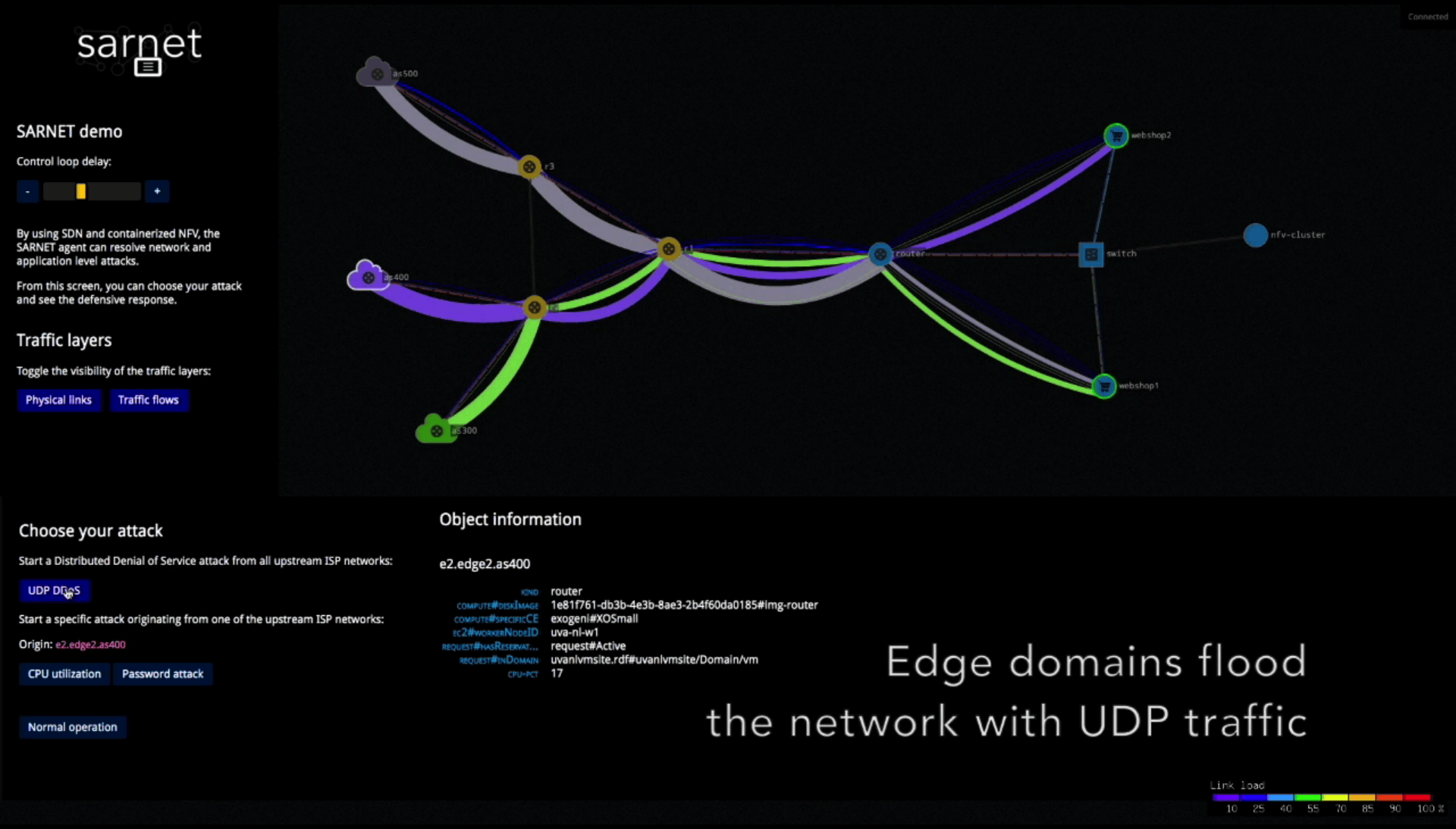
Response phase: Respond, Adjust, Measure

Learn phase: Learn (with input form other phases)

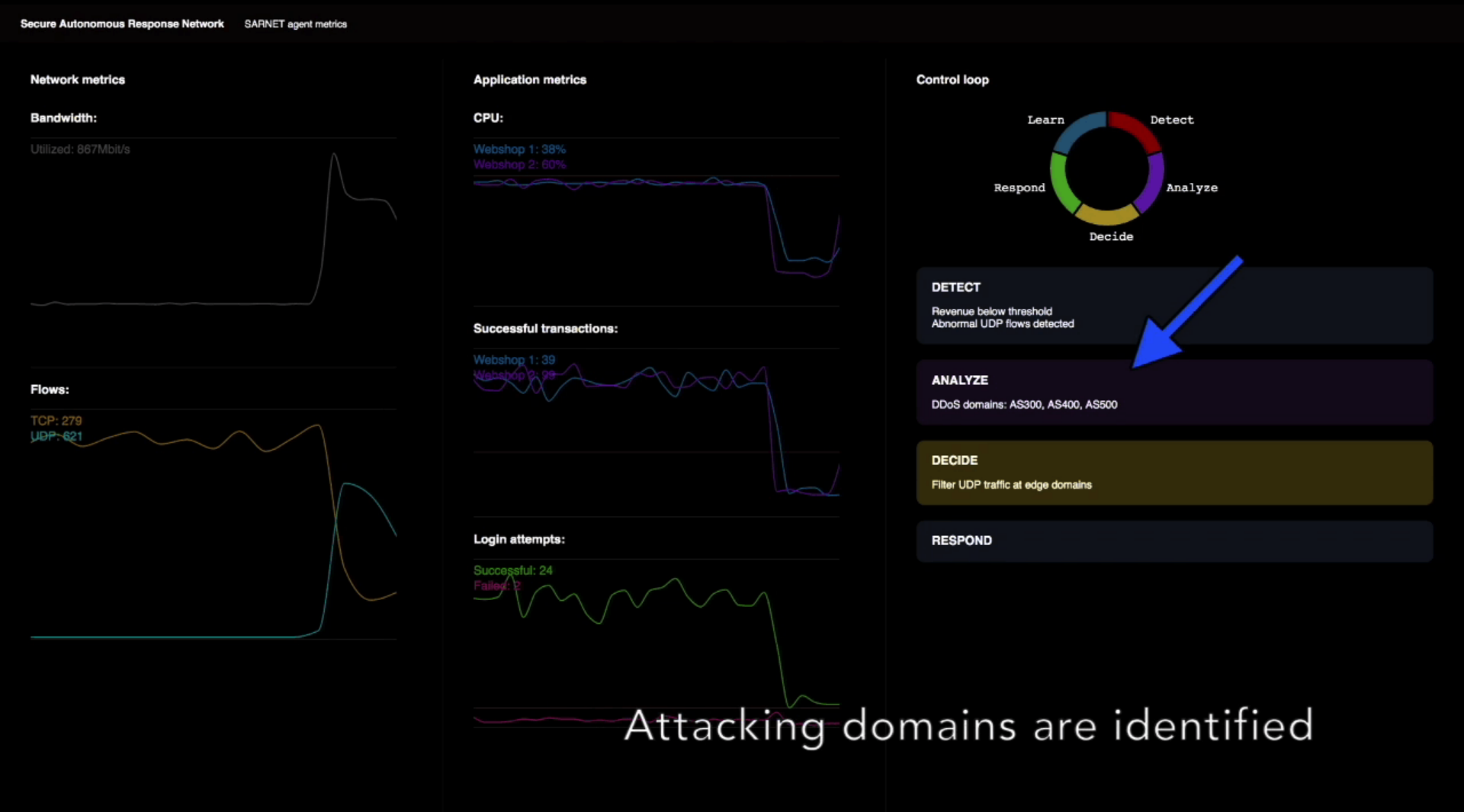
SC16 DEMO SARNET Operational Level



SC16 DEMO SARNET Operational Level

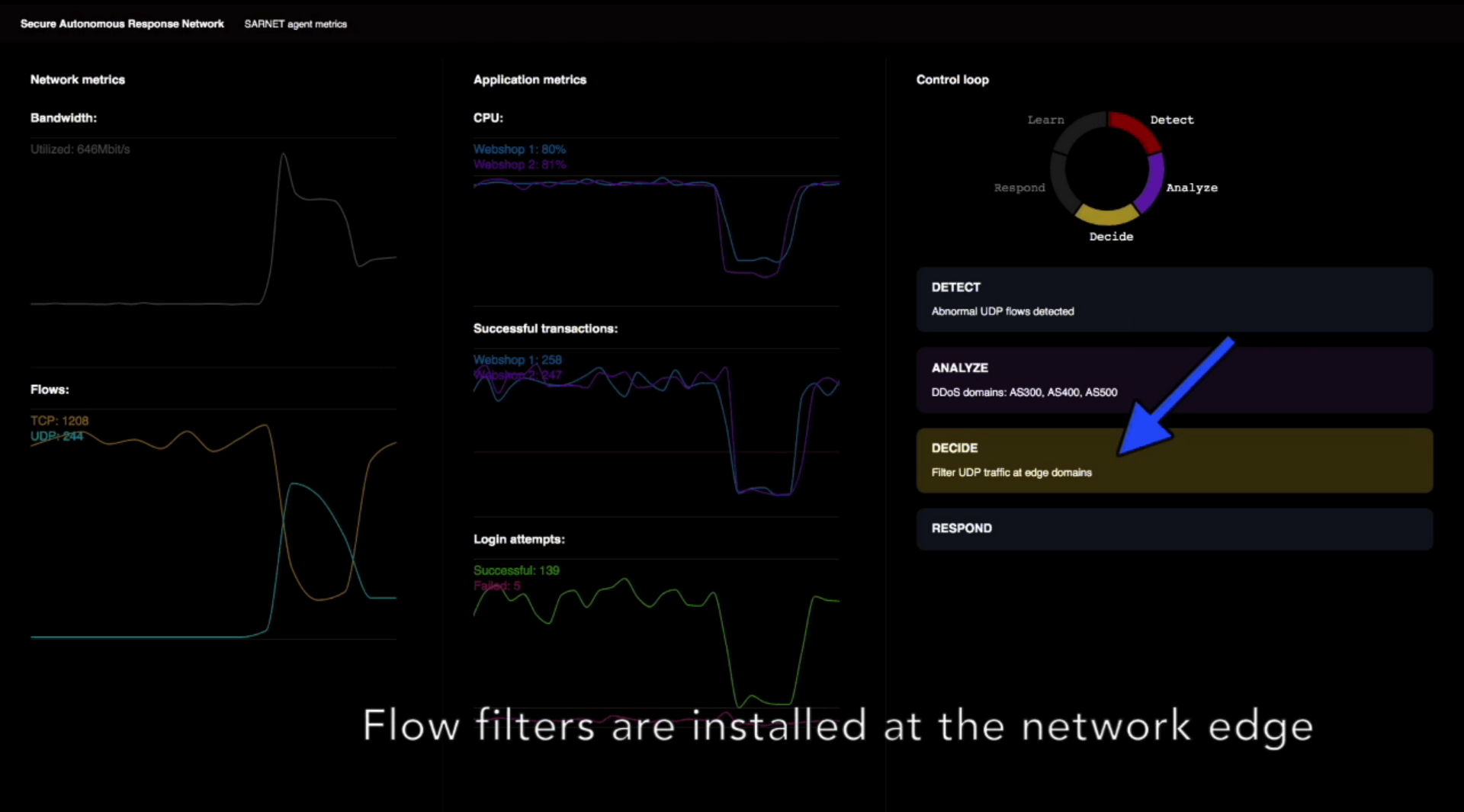


SC16 DEMO SARNET Operational Level



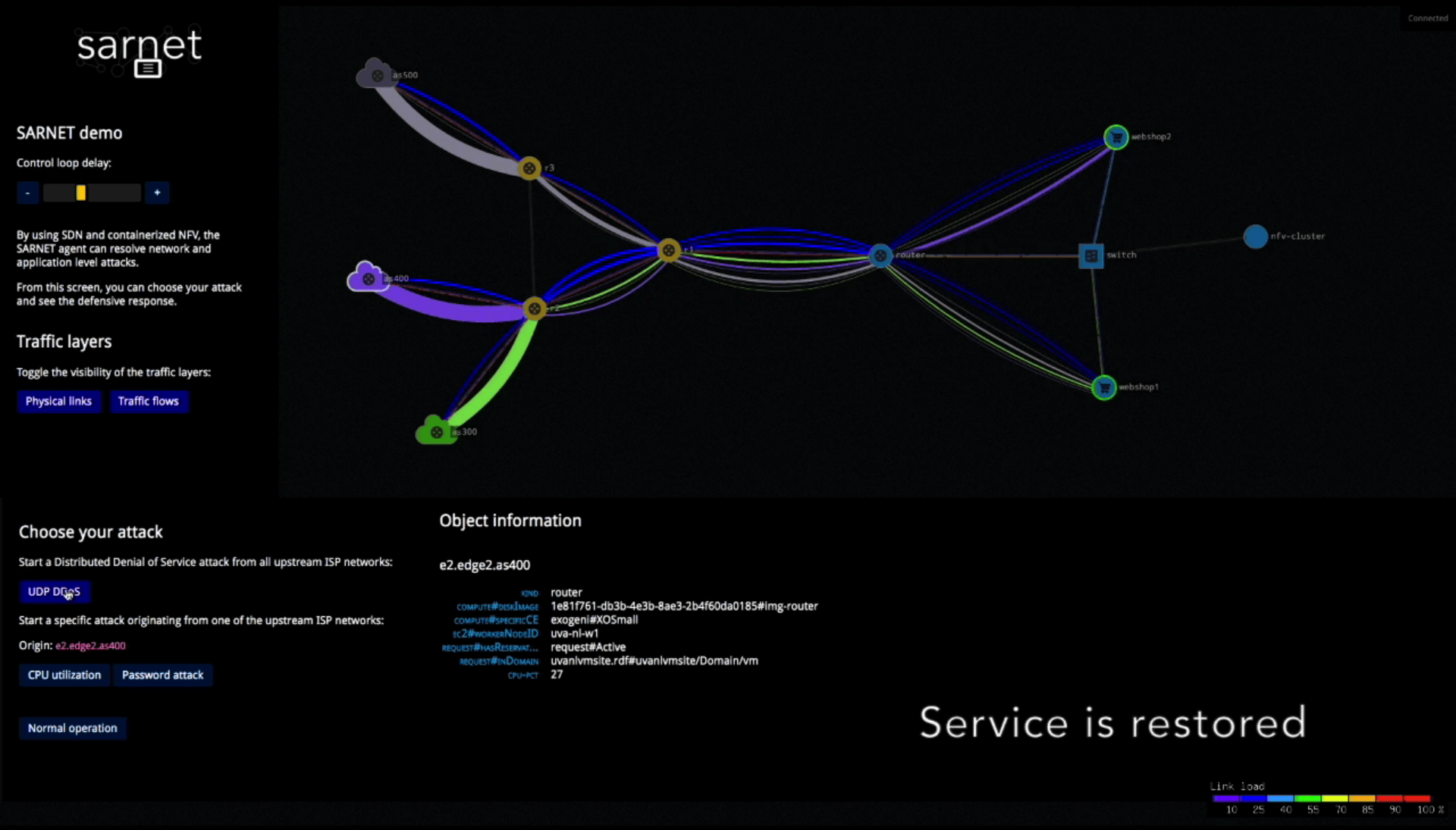
Attacking domains are identified

SC16 DEMO SARNET Operational Level

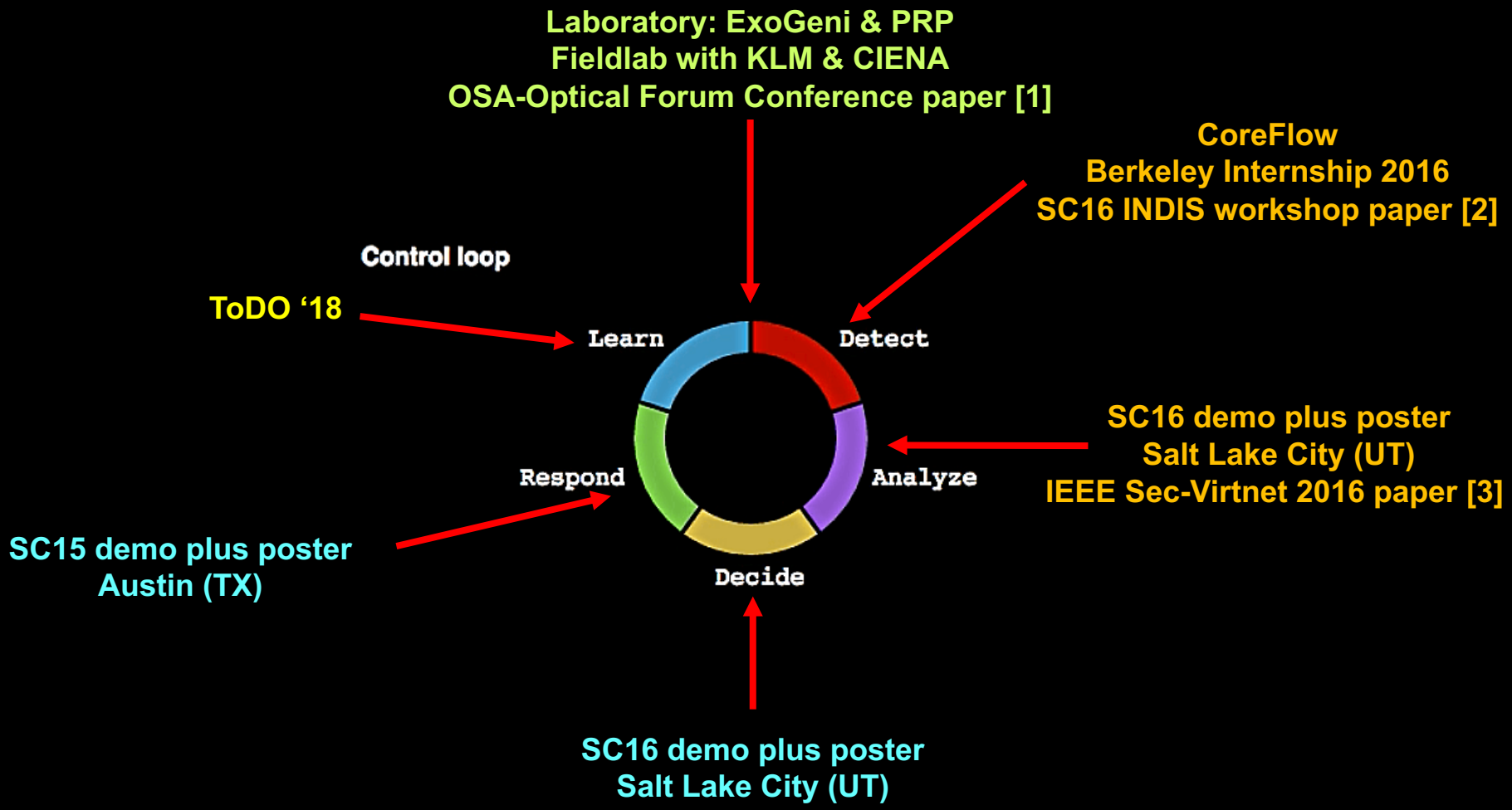


Flow filters are installed at the network edge

SC16 DEMO SARNET Operational Level



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", SC16 Salt Lake City, INDIS workshop, Nov 13, 2016.
3. Paper: Ralph Koning, Ben de Graaff, Cees de Laat, Robert Meijer, Paola Grosso, "Analysis of Software Defined Networking defences 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.

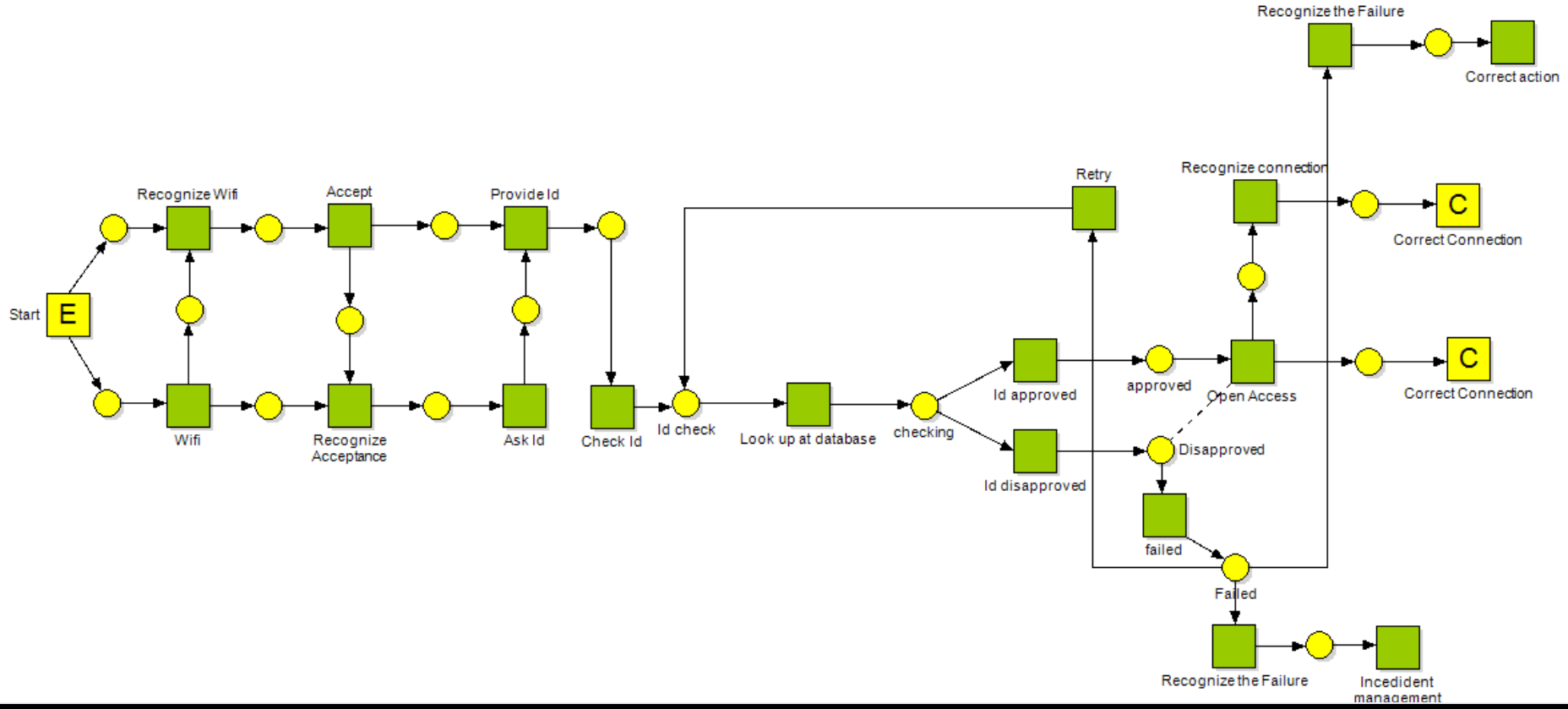
Agent Based Modelling Framework

	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:

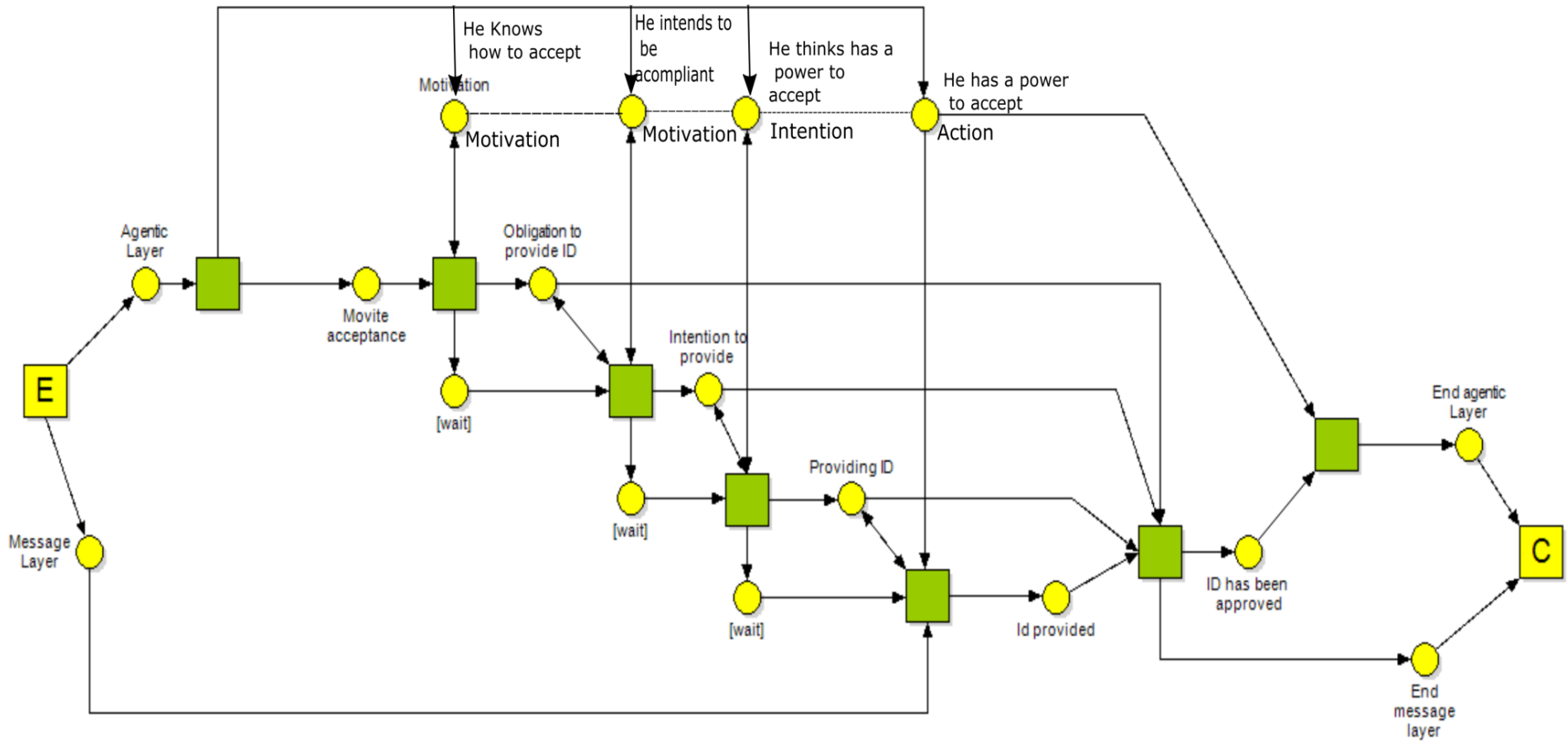
- the signal layer— describes acts, side-effects and failures showing outcomes of actions in a topology.
- the action layer—actions: performances that bring a certain result,
- the intentional layer—intentions: commitments to actions, or to build up intentions,
- the motivational layer—motives: events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

Simplified Eduroam case at signalling layer



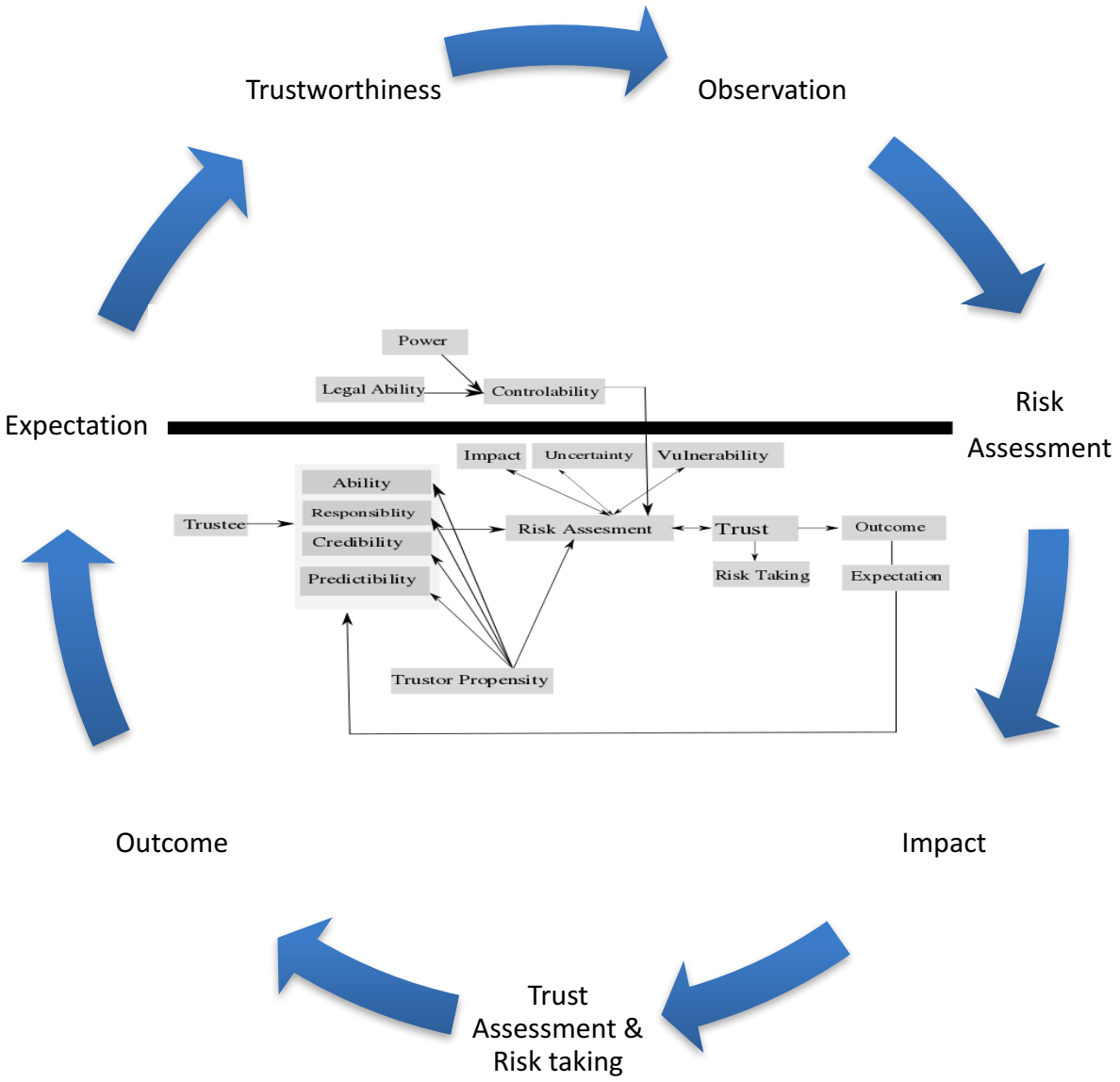
Petri net of EduRoam Case
(first step)

Describing Intentions, Motivations and Actions

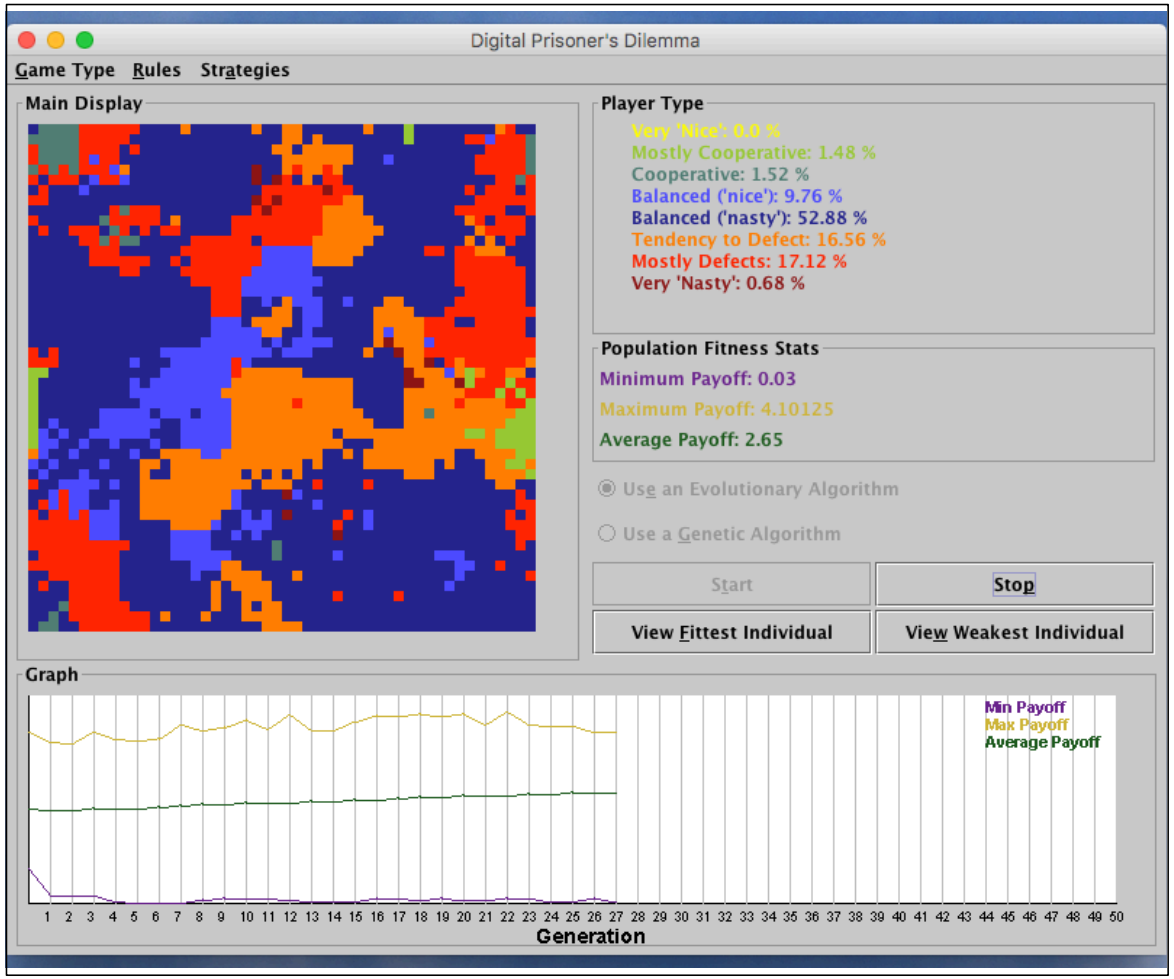


Petri net of EduRoam Case

Agent Model evaluating Trust



First step: Evolutionary Prisoners Dilemma using ABM Simulation



Agents choose from different strategies:

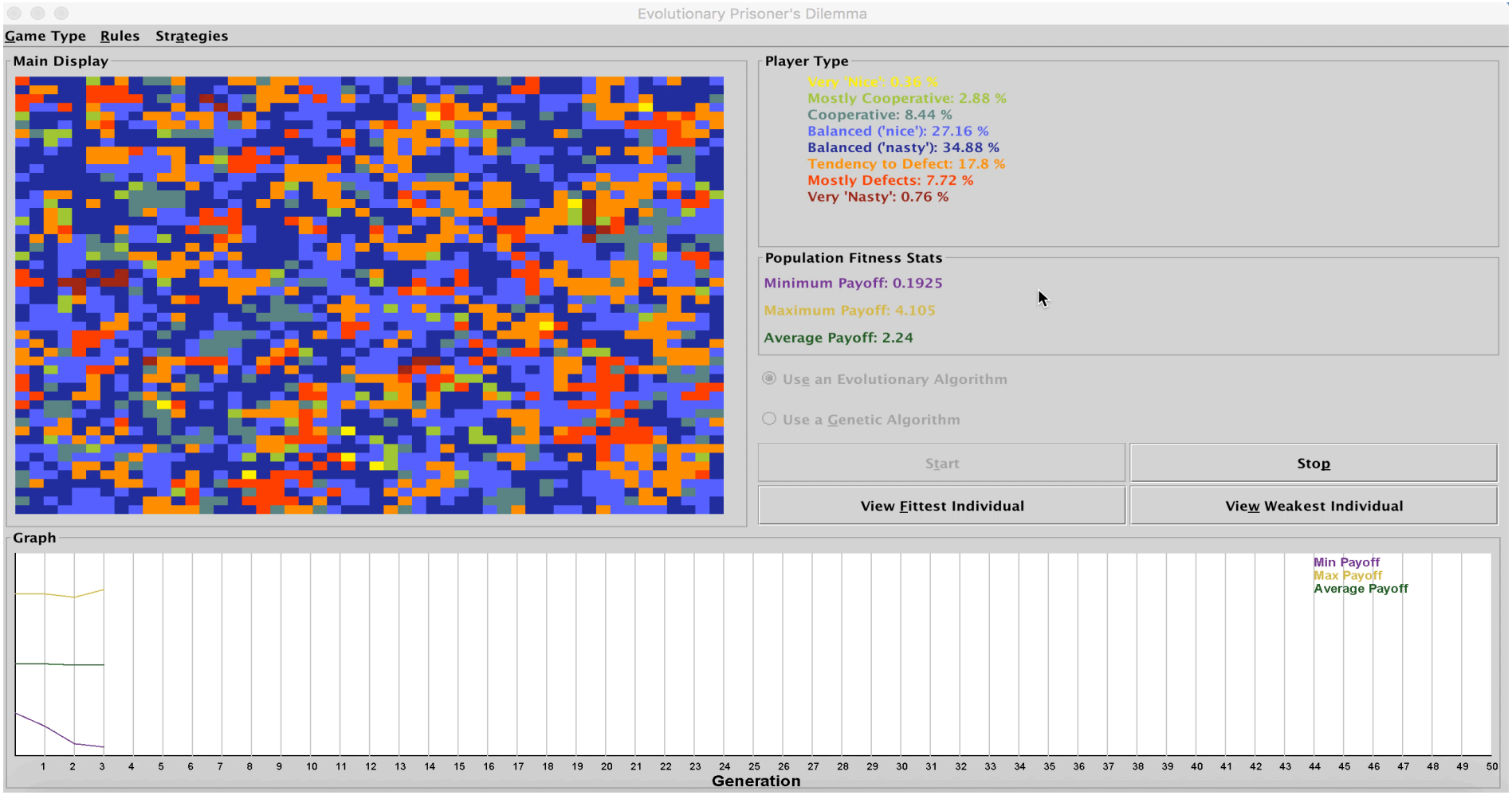
- Collaborate
- Defect
- During simulation: Agents predict next behavior of neighboring agents learned from observing past behavior.

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.

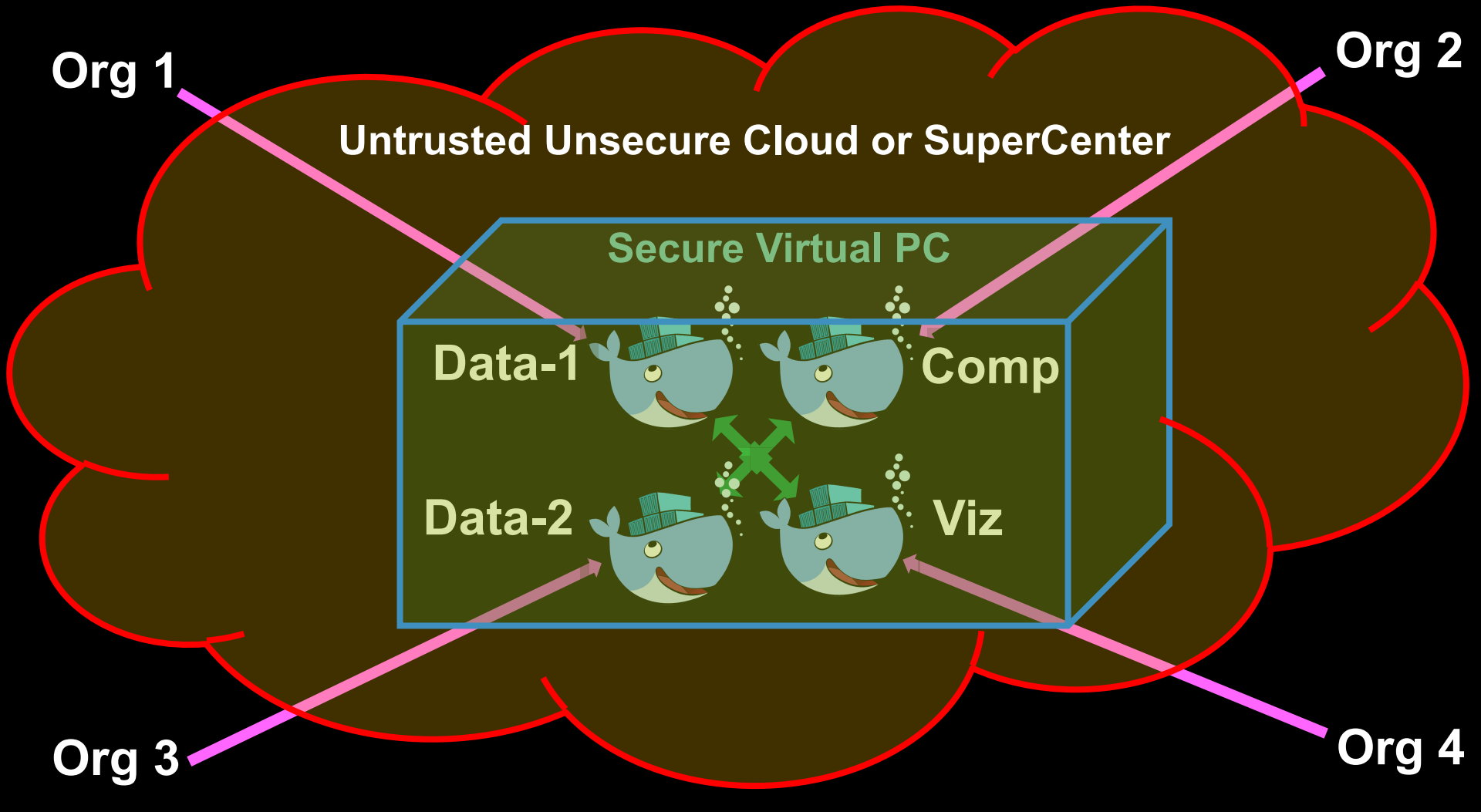
Research performed by Ameneh Deljoo, PhD candidate University of Amsterdam.

ABM Simulation



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 encryped hard drive)
- Compute Docker (protected application, signed algorithms)
- Visualization Docker (to visualize output)



Next steps

- Auto-tune detectors
- Machine Learning
- Put entire SARNET demo in VM
- Distribute flocks of VM's playing different roles
- Study multi domain challenges
- Study stability of SARNETS
- See you at SC17 in DENVER!

Q & A



NWO
Netherlands Organisation
for Scientific Research

COMMIT/

ciena

TNO

AIRFRANCE KLM