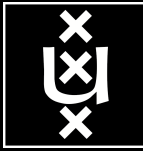


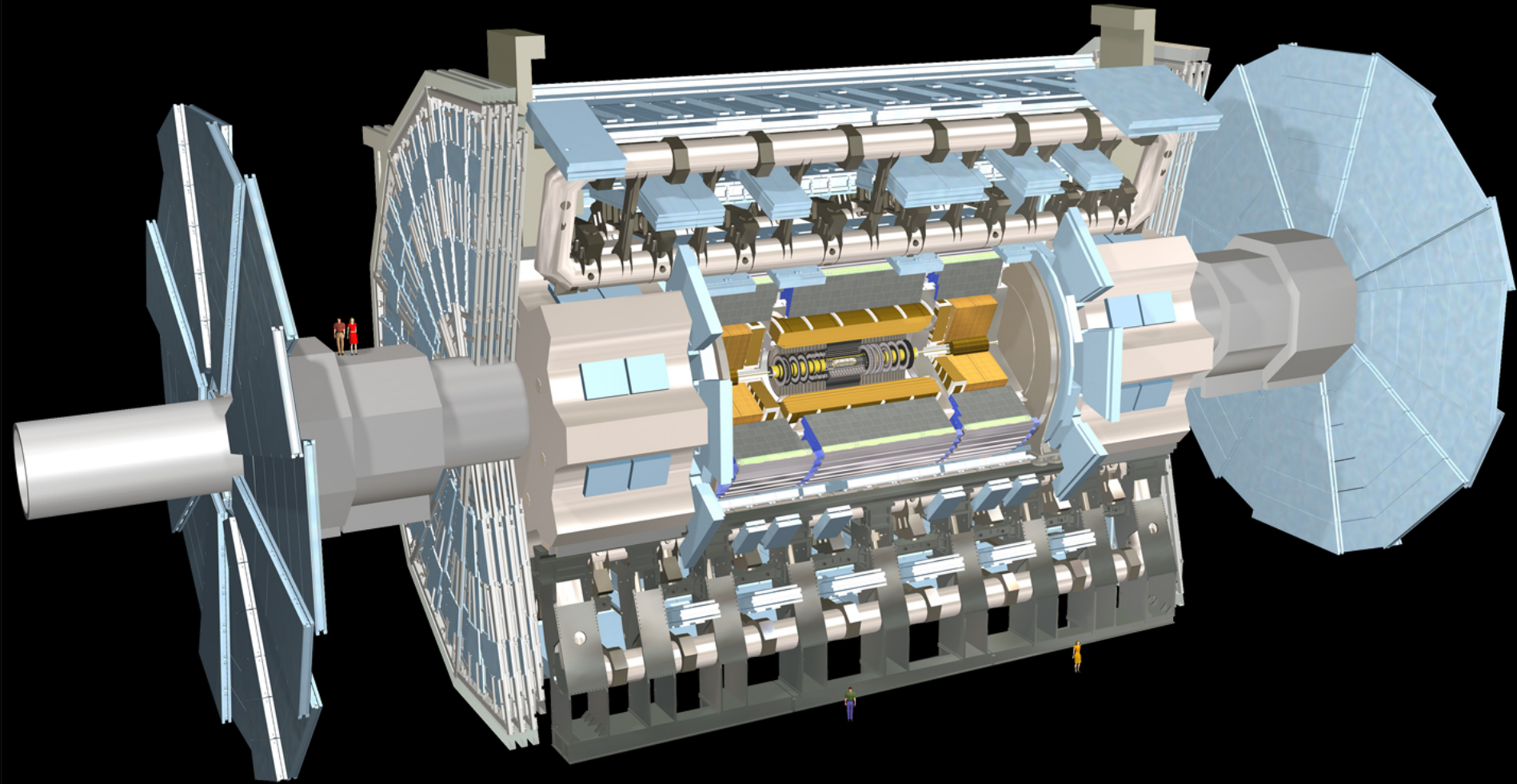
Enabling E-Science Applications with Dynamic Optical Networks: Secure Autonomous Response Networks.

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





What Happens in an Internet Minute?

1,572,877 GB of global IP data transferred¹

10 Million ads displayed²

347,222 Tweets³

3.3 Million pieces of content shared⁴

6.9 Million messages sent⁴

Netflix + Youtube = more than 1/2 of all traffic⁵

438,801 Wiki page views⁷

\$400 Million during Alibaba peak day sales⁶

10 Million WeChat messages at its peak⁹

34.7 Million instant messages (MIM) sent⁸

194,064 app downloads¹⁰

\$133,436 in sales¹¹

31,773 hours of music played¹²

38,194 photos uploaded¹³

57,870 page views¹⁴

4.1 Million searches¹⁵

100 hours of video uploaded¹⁶

138,889 hours of video watched¹⁶

23,148 hours of video watched¹⁷

And Future Growth is Staggering



By 2017, mobile traffic will have grown **13X** in just 5 years¹



In 2017, there will be **3X** more connected devices than people on Earth¹

All digital data created reached **4 zettabytes** in 2013¹⁸

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



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

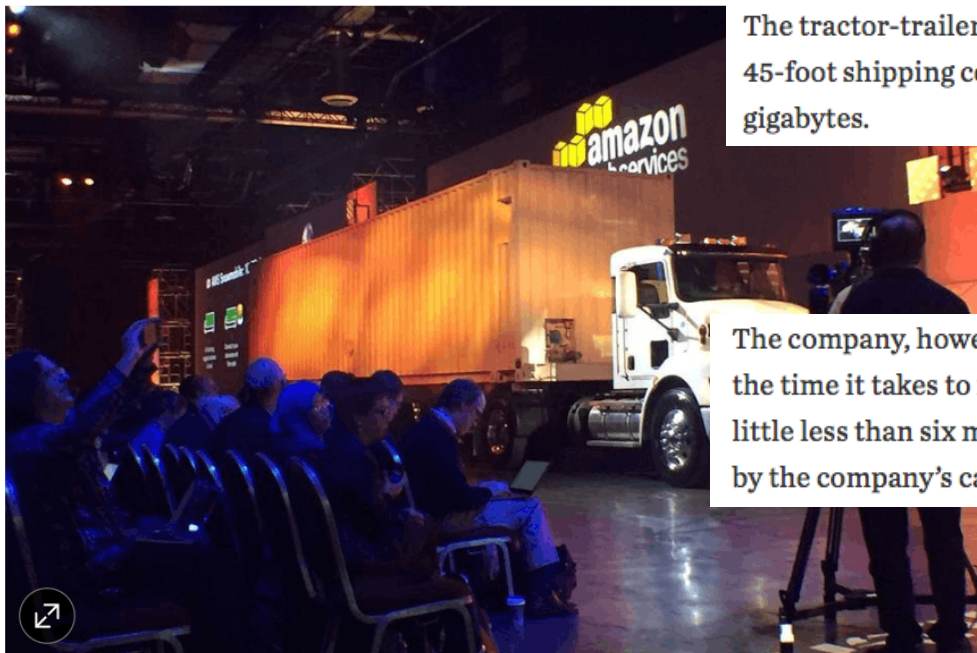


Netflix Now Lets You Download, But Many Top Shows Are Off Limits

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

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.

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.

1 fiber does about 16 Tbit/s
= 2 Tbyte/s
⇒ 50000 s/ExaByte
⇒ One week/ExaByte

Out

2. What Are Clothes

3. Opinion The Rev

Most Popular

1. U.S. to Po Least \$10 Student Coming

2. Opinion: Trump's Pick Sca

3. Trump's His Busi Draws Q

4. Creator of Mac Dies

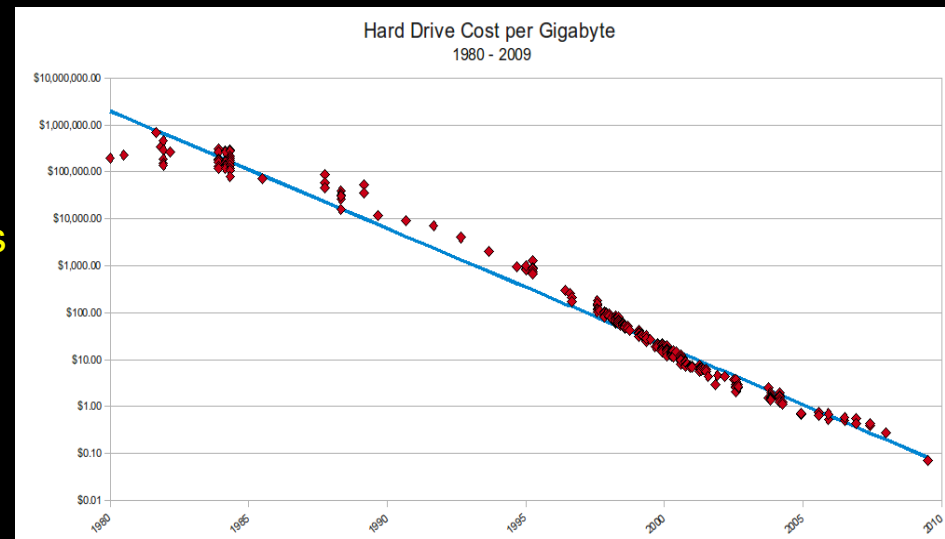
5. Trump's Choice S Absolute

Moore's and Kryders Law

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

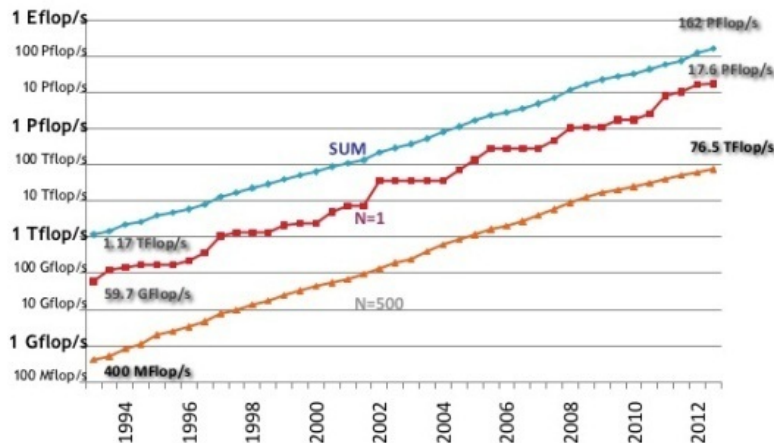
- A virus, a hacker, or a system failure can instantly send digital shockwaves around the world.

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.



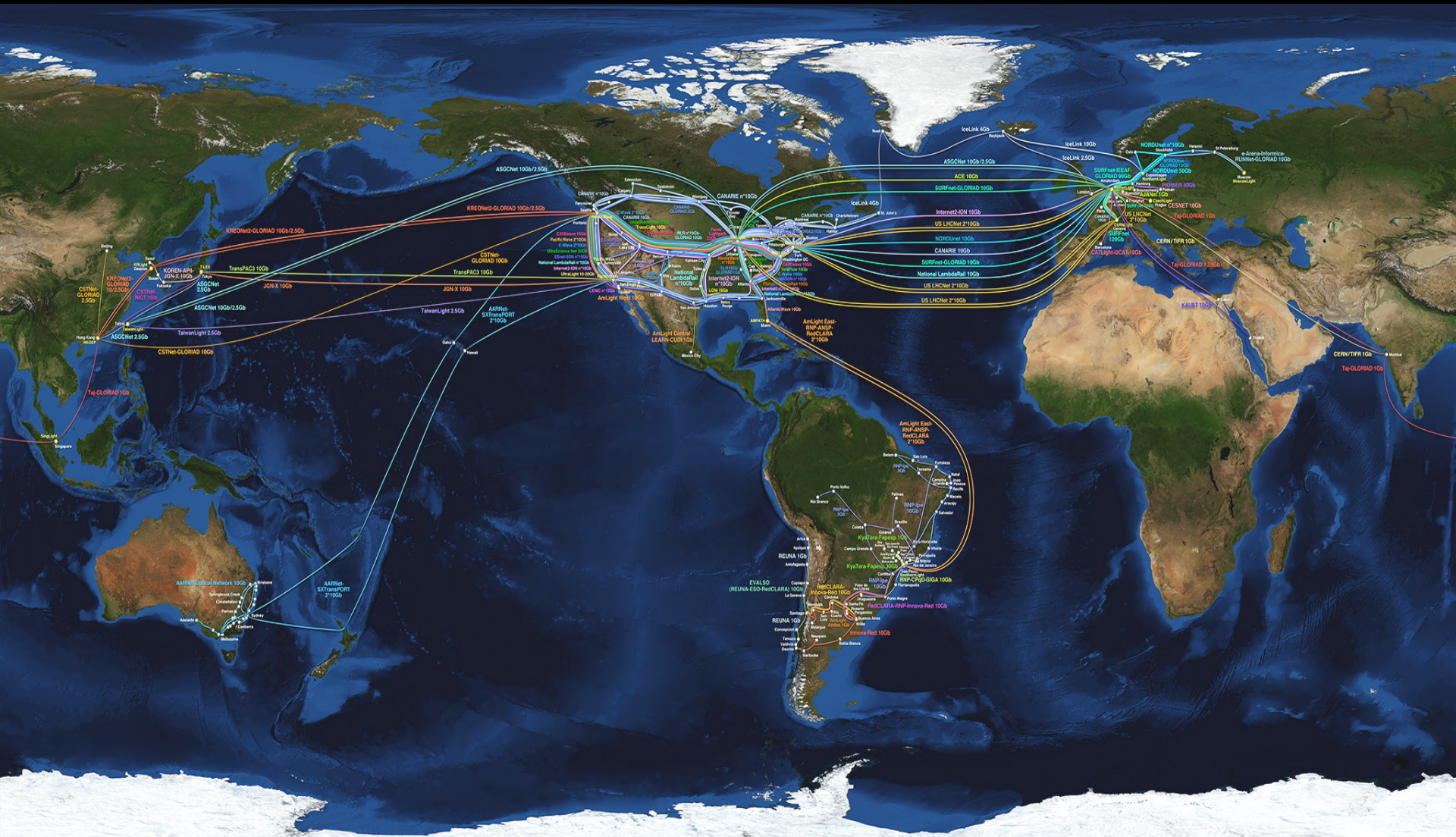
We will soon reach the limits of what is currently feasible and controllable.

Performance Development



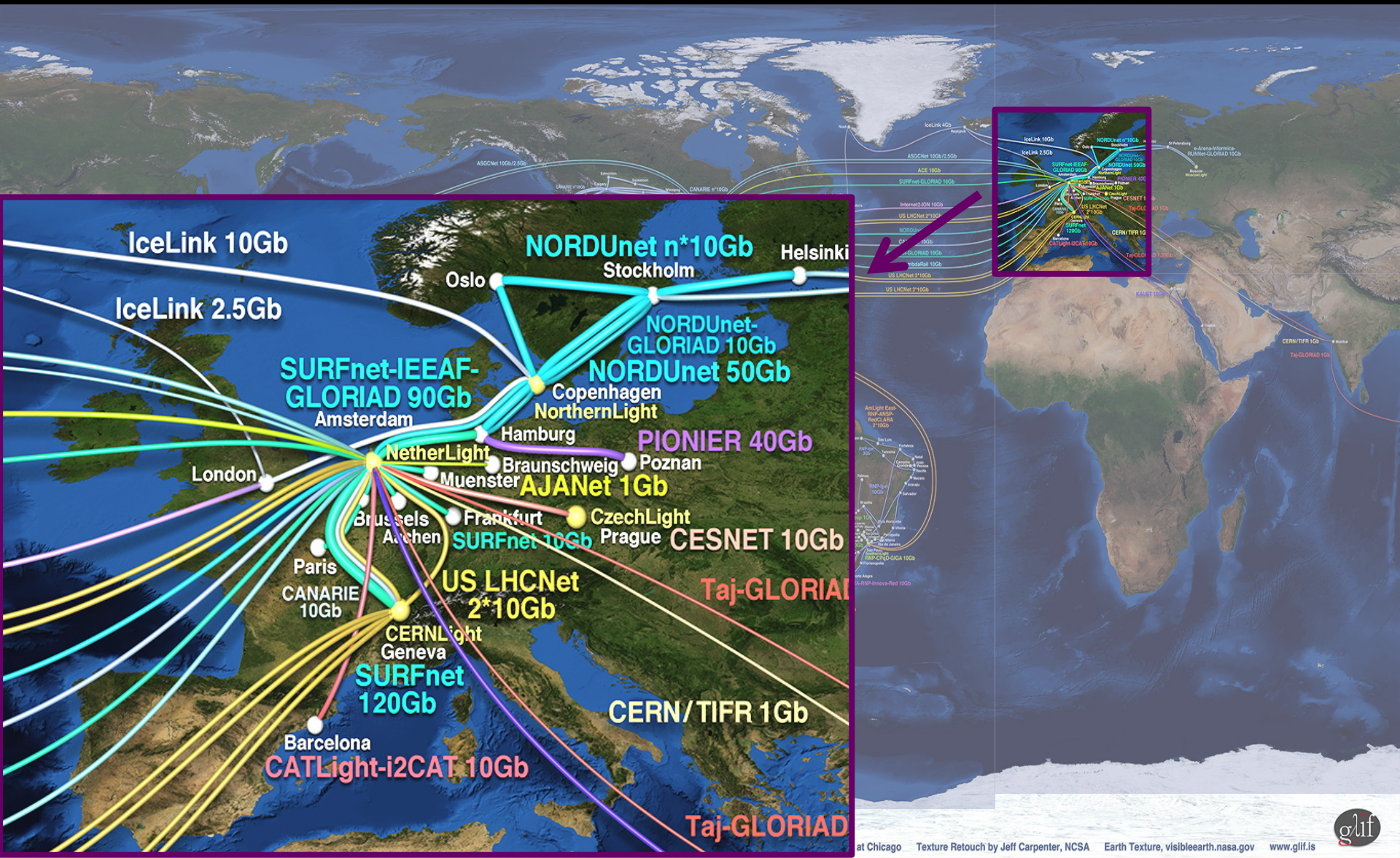
The GLIF – LightPaths around the World

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

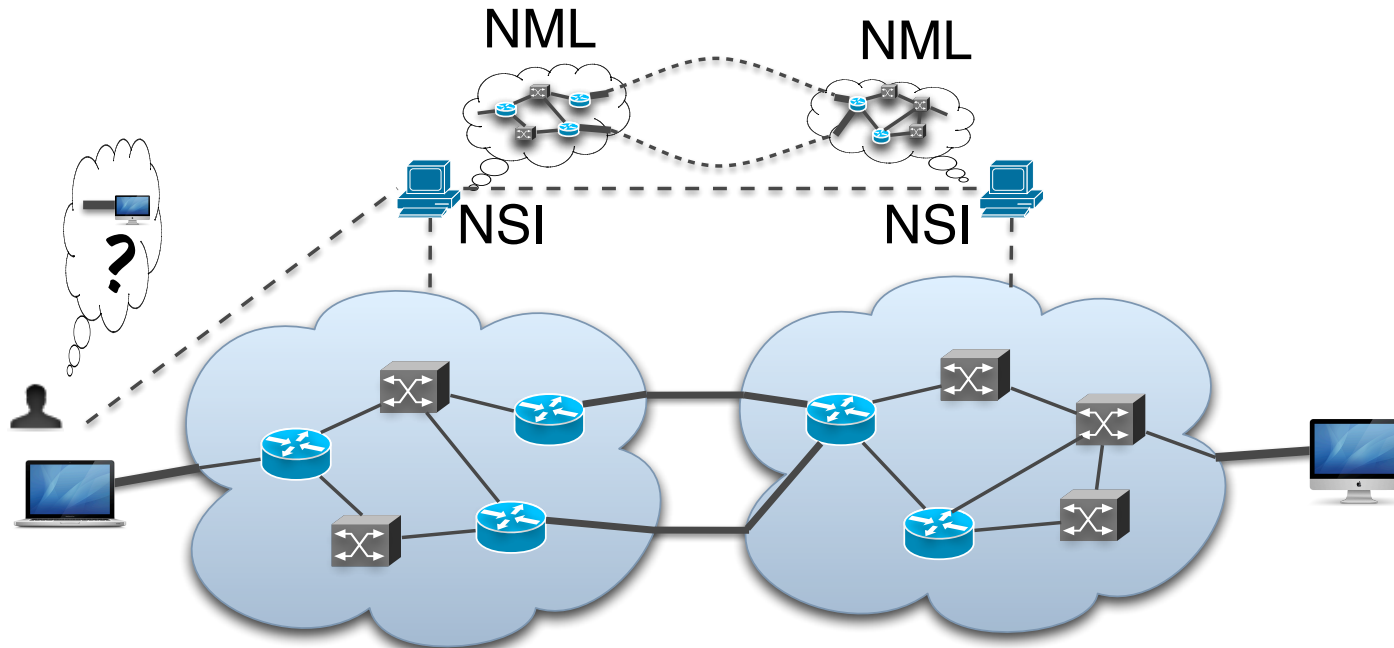
F Dijkstra, J van der Ham, P Grosso, C de Laat, "A path finding implementation for multi-layer networks", Future Generation Computer Systems 25 (2), 142-146.



Network Topology Description

Network topology research supporting automatic network provisioning

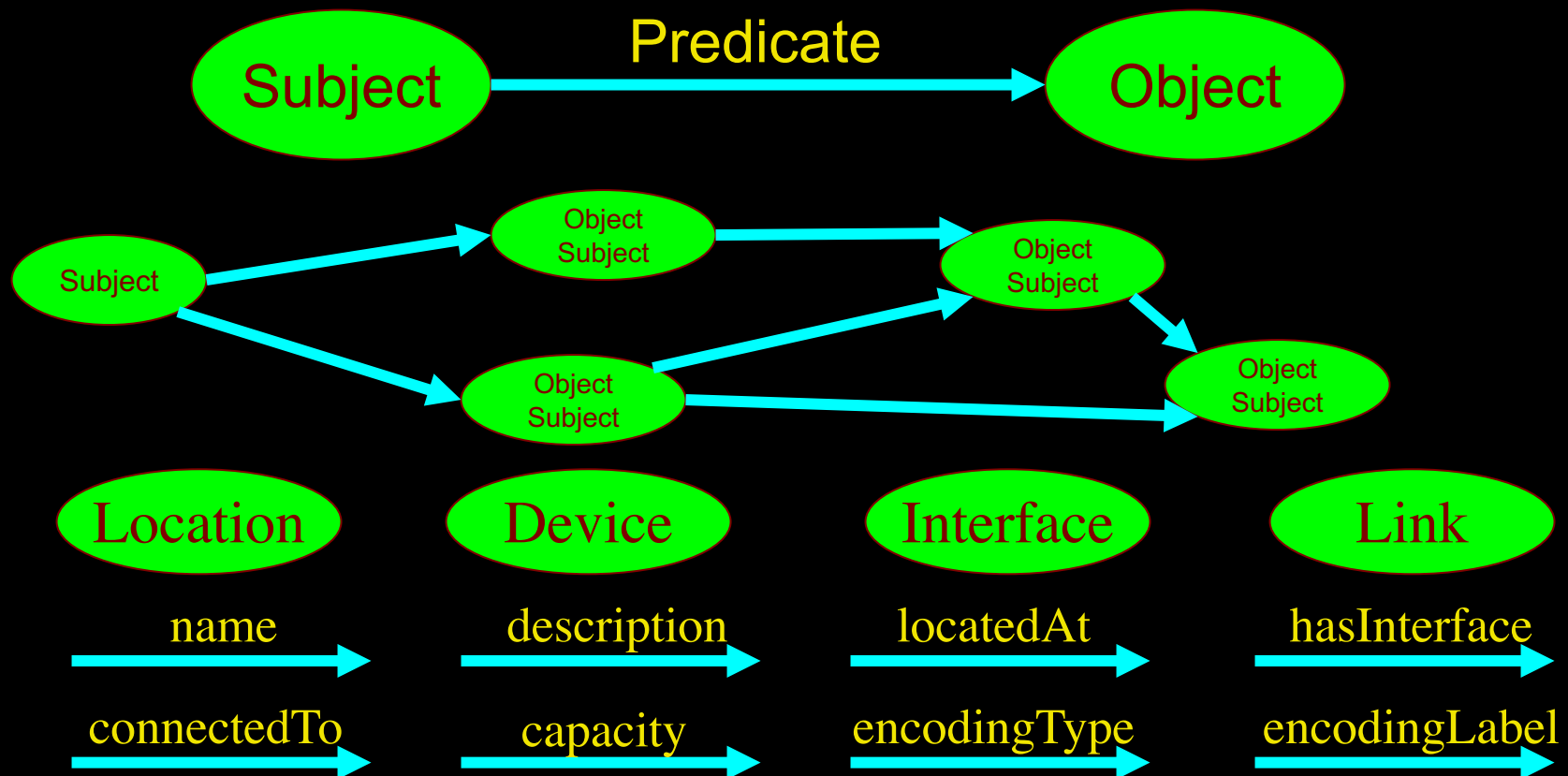
- Inter-domain networks
- Multiple technologies
- Based on incomplete information
- Possibly linked to other resources



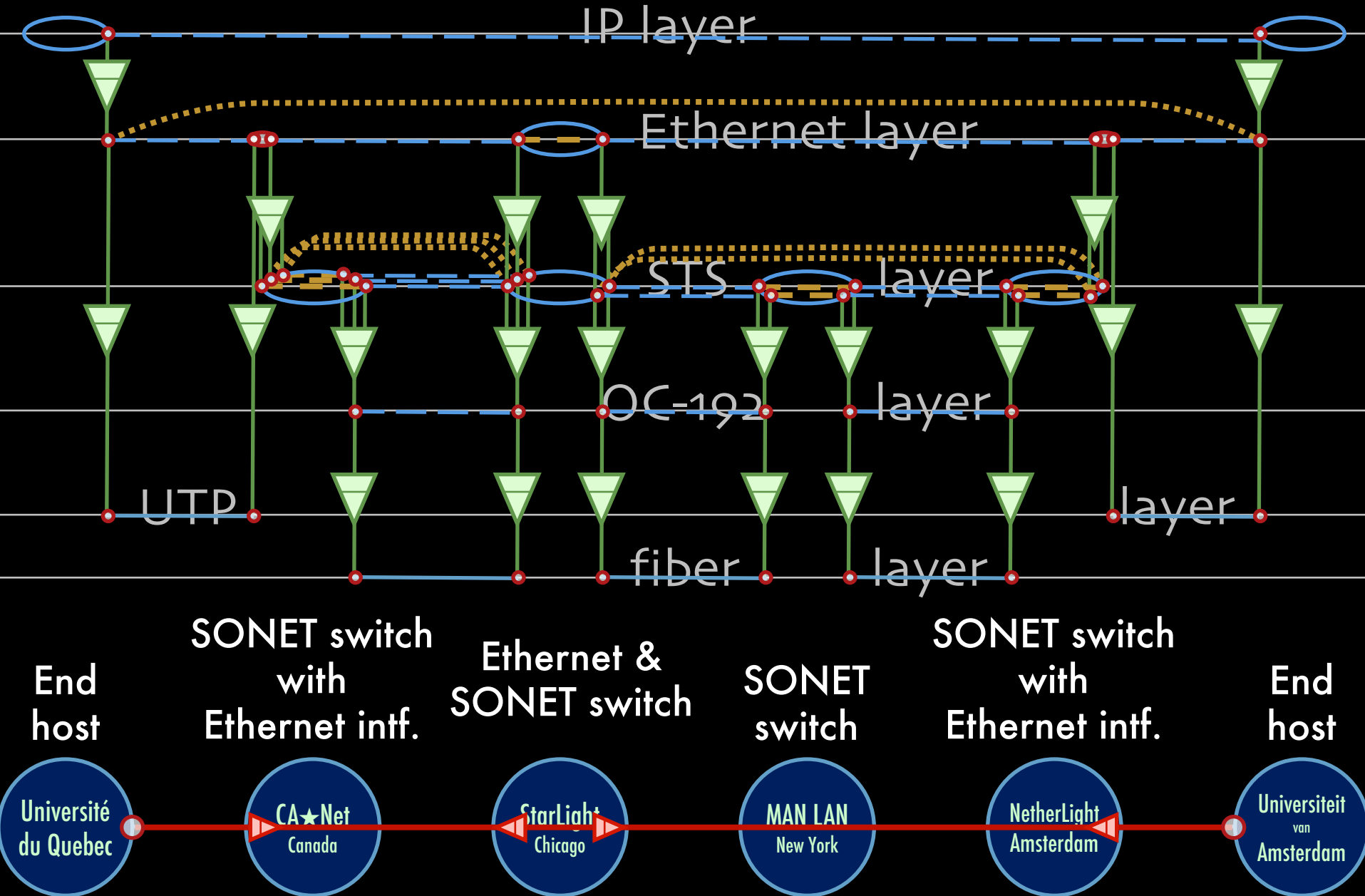
LinkedIn for Infrastructure - iNDL



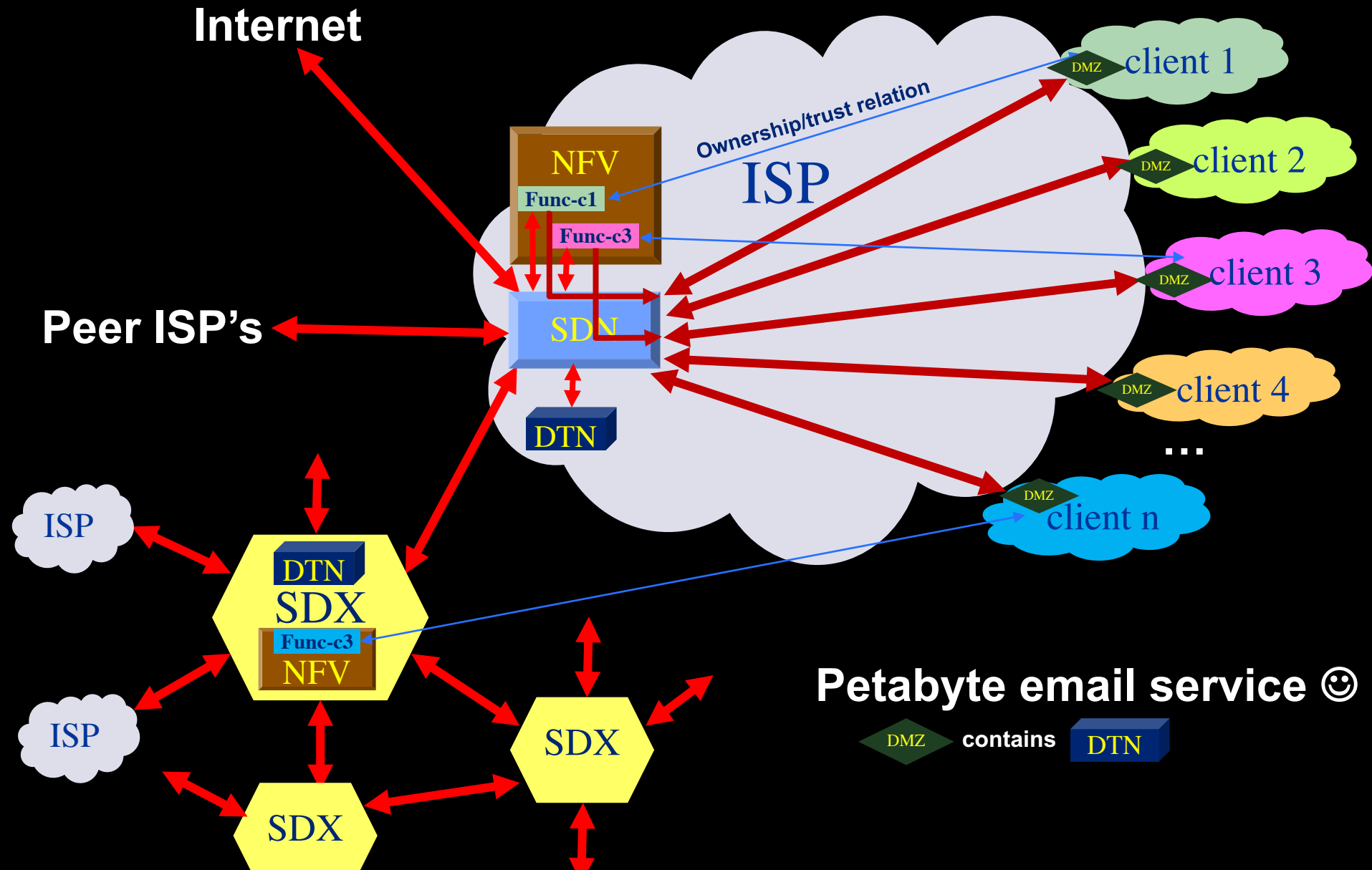
- From semantic Web / Resource Description Framework.
- The RDF uses XML as an interchange syntax.
- Data is described by triplets (Friend of a Friend):

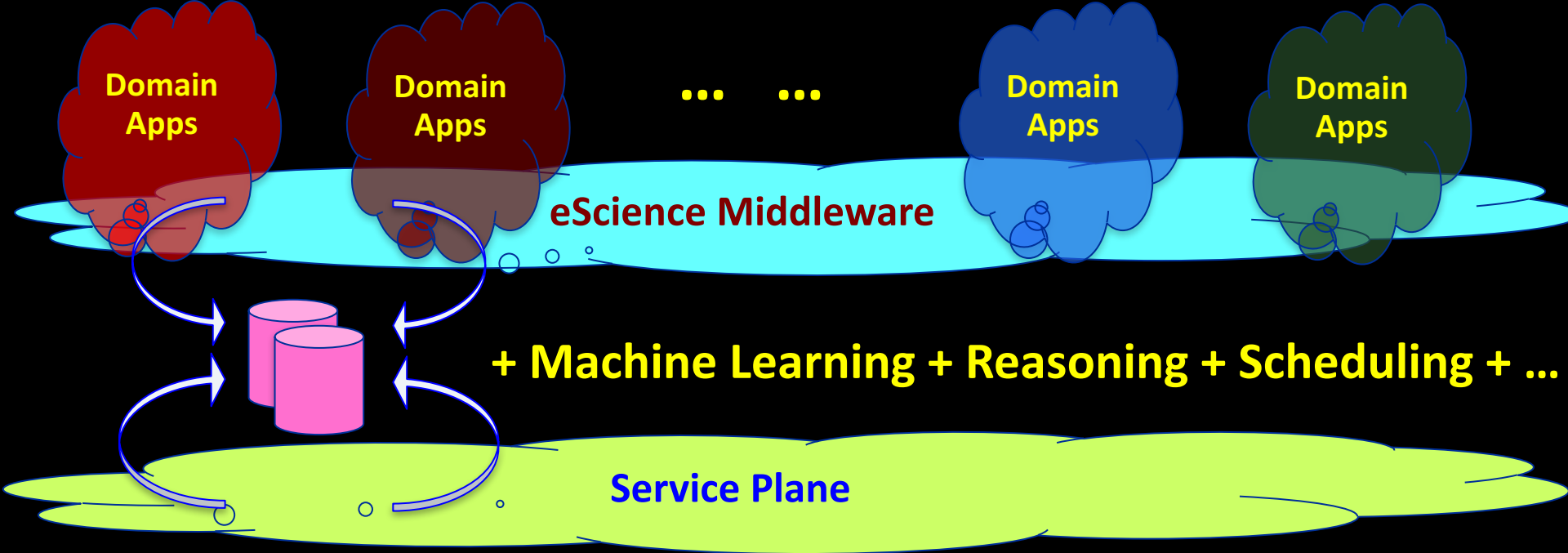


Multi-layer descriptions in NDL

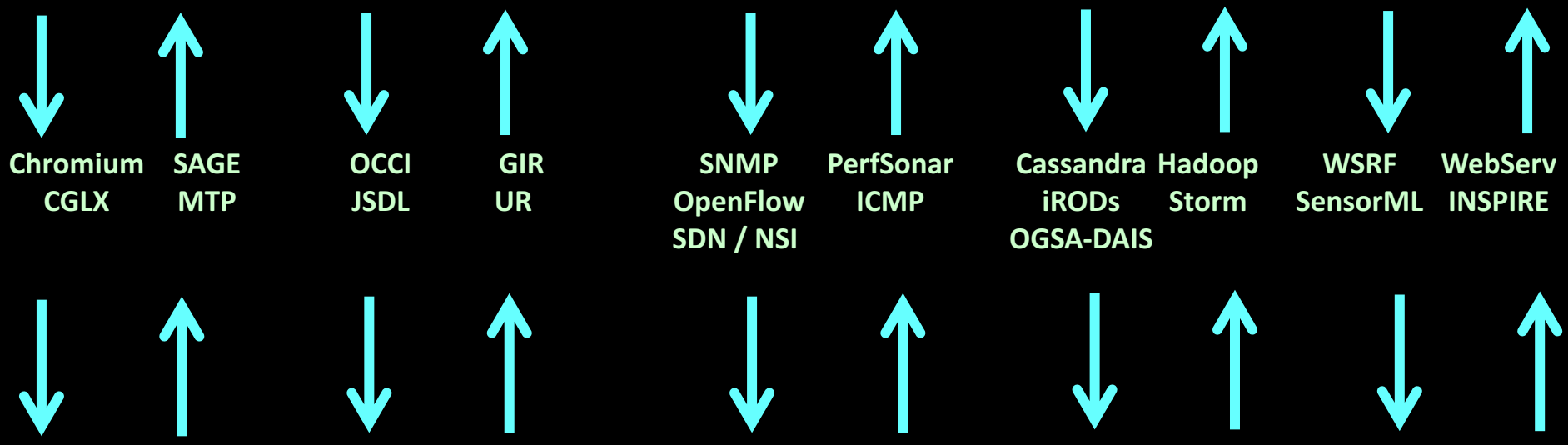


Networks of ScienceDMZ's & SDX's

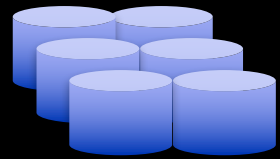
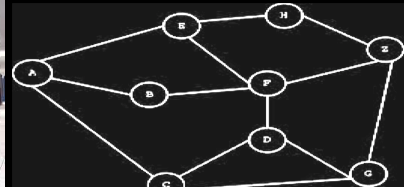




+ Machine Learning + Reasoning + Scheduling + ...



GRID/Cloud Computing



Basic operating system loop

The image shows a web browser window displaying a network simulation interface. The browser address bar shows `localhost:4567/vi/7`. The page content includes a navigation menu with items like `netapps (provider, zone)` and `connections`. A sidebar on the left lists various modes and actions such as `info`, `info edge`, `draw`, `delete node`, and `delete edge`. The main area features a network graph with nodes labeled with IDs like `13124`, `13127`, `13128`, `13125`, and `13126`. Below the graph, there are radio buttons for selecting different zones and a 'Create generator' section with a list of parameters.

On the right side, a terminal window displays Mathematica code for graph analysis. The code includes functions for `Bicomponents`, `ArticulationVertices`, and `GraphPlot`. The `Bicomponents` function is defined as:

```
Bicomponents[n_]:=Module[{v=VertexDegree[n], vl=VertexList[n]}, If[Length[n]<=1, Return[{}]; Length[n]>1, Take[n, 2]; Intersection@@c; Length[#]>0, Delete[c, Position[n, #][[1]]], #<=]; Map[First, Map[Sort[n, v[[Position[v1, #][[1]]]<v[[Position[v1, #2][[1]]]&], #], #]; geQ[n, UndirectedEdge[edge[[1]], edge[[2]]], #]; Map[Last, Map[Sort[n, v[[Position[v1, #][[1]]]<v[[Position[v1, #2][[1]]]&], #], #]]];
```

The `ArticulationVertices` function is defined as:

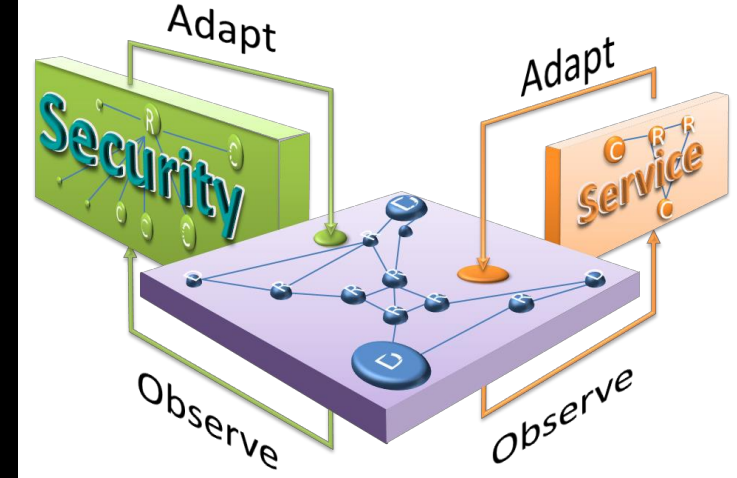
```
ArticulationVertices[n_]:=Module[{v=VertexDegree[n], vl=VertexList[n]}, {Bicomponents[n], Function[{x}, Total[v[[Position[v1, #][[1]]]&/@x][[#1]]<Function[{x}, Total[v[[Position[v1, #][[1]]]&/@x][[#2]]&], n]}];
```

Below the terminal, there are several smaller panels showing network diagrams and code snippets. One panel shows a simple graph with nodes 1 and 2. Another panel shows a cycle graph with 7 nodes. A third panel shows a network with nodes 1 through 6 and their connections.

Cyber security program SARNET

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

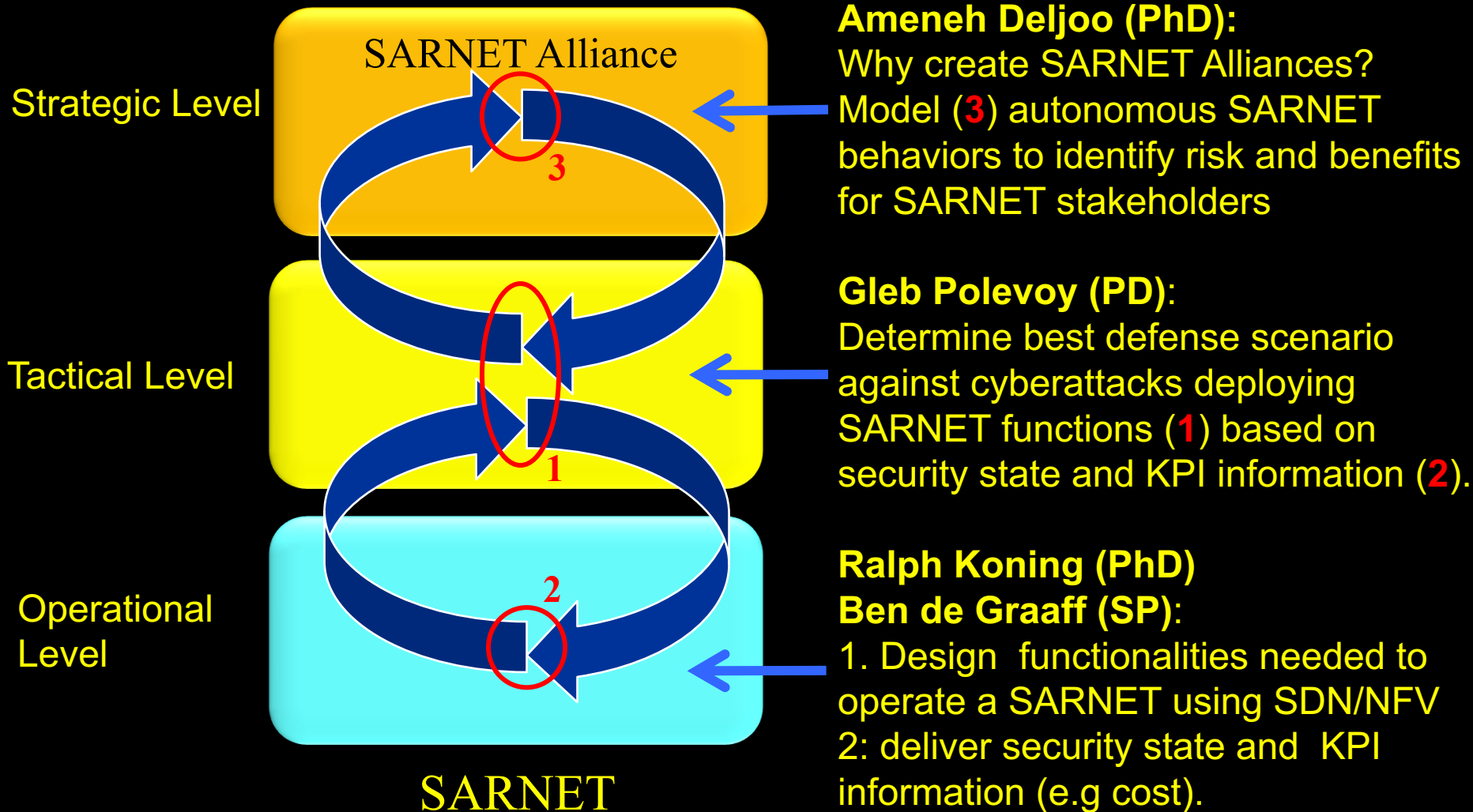
- model their state (situation)
- discover by observations and reasoning if and how an attack is developing and calculate the associated risks
- have the knowledge to calculate the effect of counter measures on states and their risks
- choose and execute one.



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

Context & Goal

Security Autonomous Response NETWORK Research

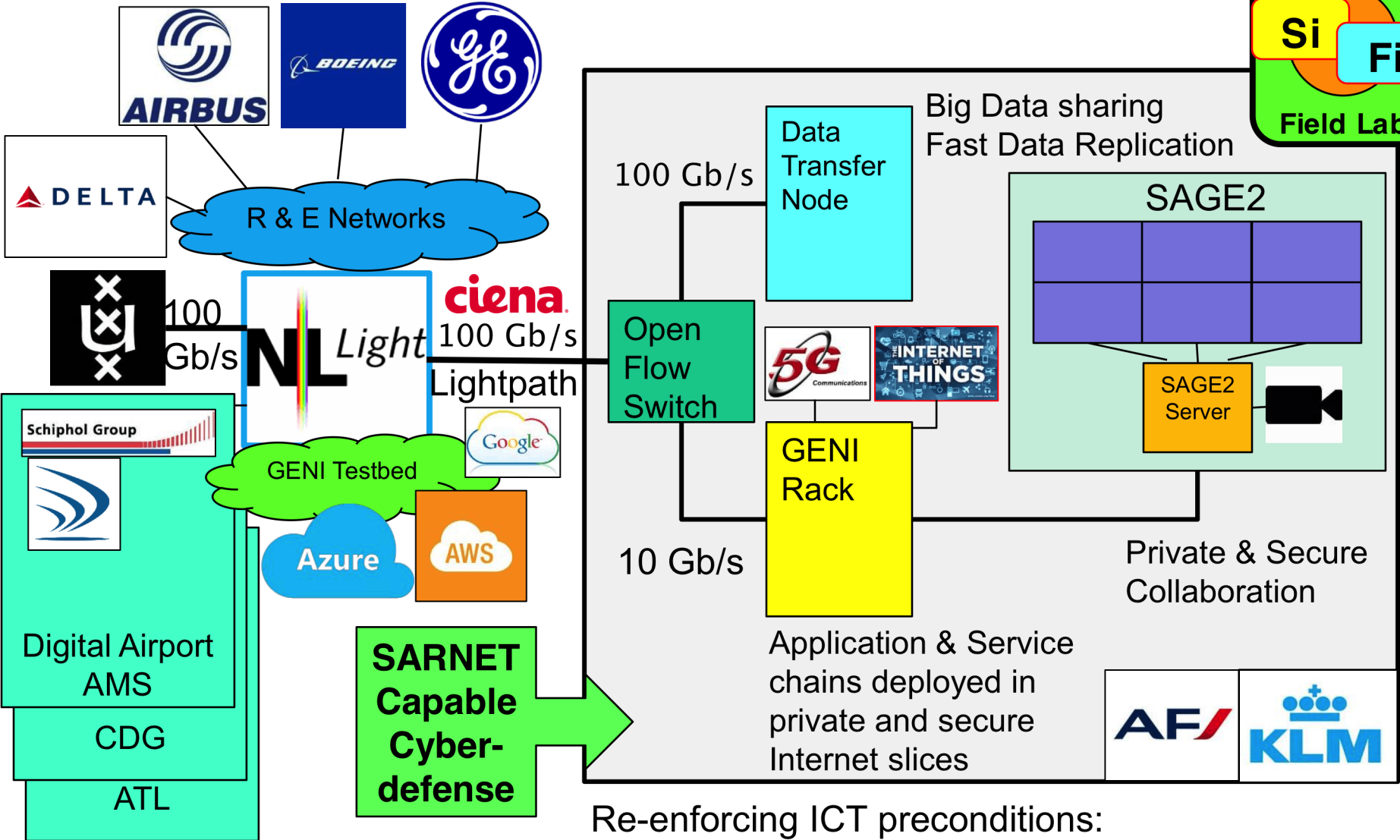
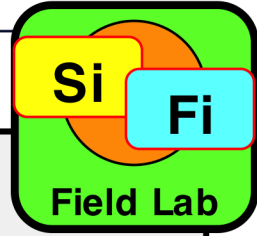


Ameneh Deljoo (PhD):
Why create SARNET Alliances?
Model (3) autonomous SARNET behaviors to identify risk and benefits for SARNET stakeholders

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

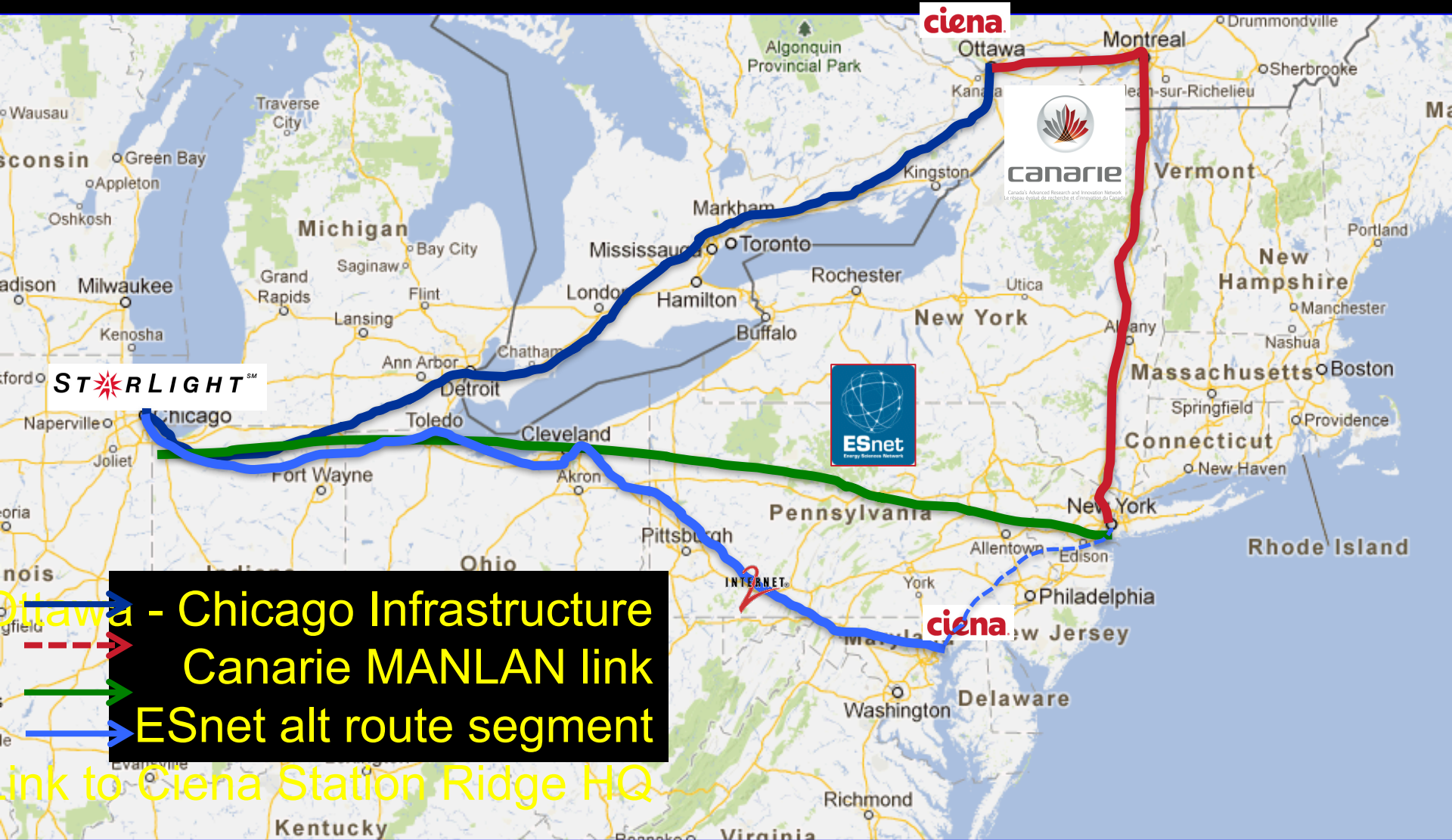
Ralph Koning (PhD)
Ben de Graaff (SP):
1. Design functionalities needed to operate a SARNET using SDN/NFV
2: deliver security state and KPI information (e.g. cost).

Ambition to put capabilities into fieldlab



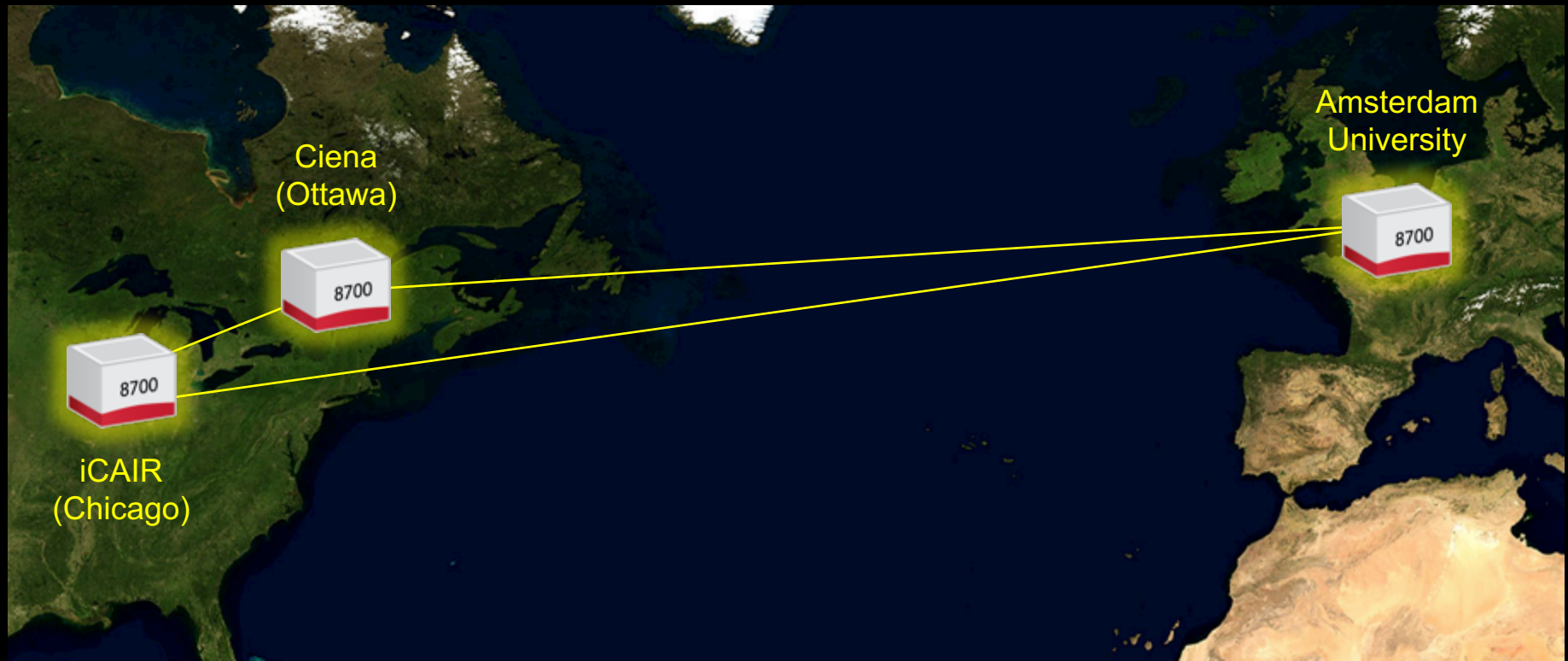
Re-enforcing ICT preconditions:
Each envisaged site has similar elements

Ciena's CENI topology



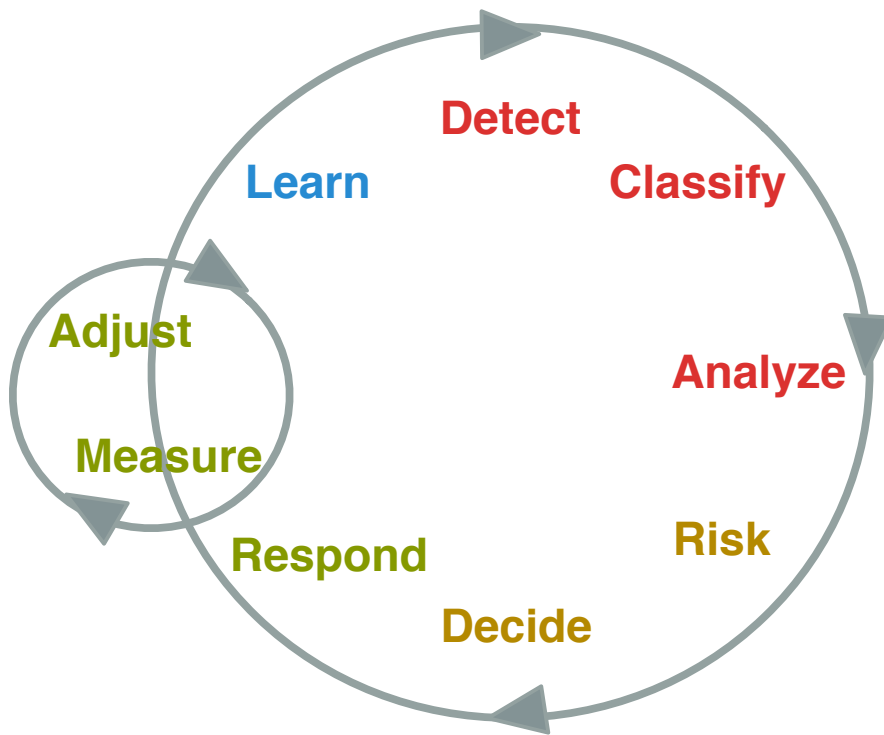
CENI, International extension to University of Amsterdam

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.

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

sarnet

Connected

SARNET demo

Control loop delay:



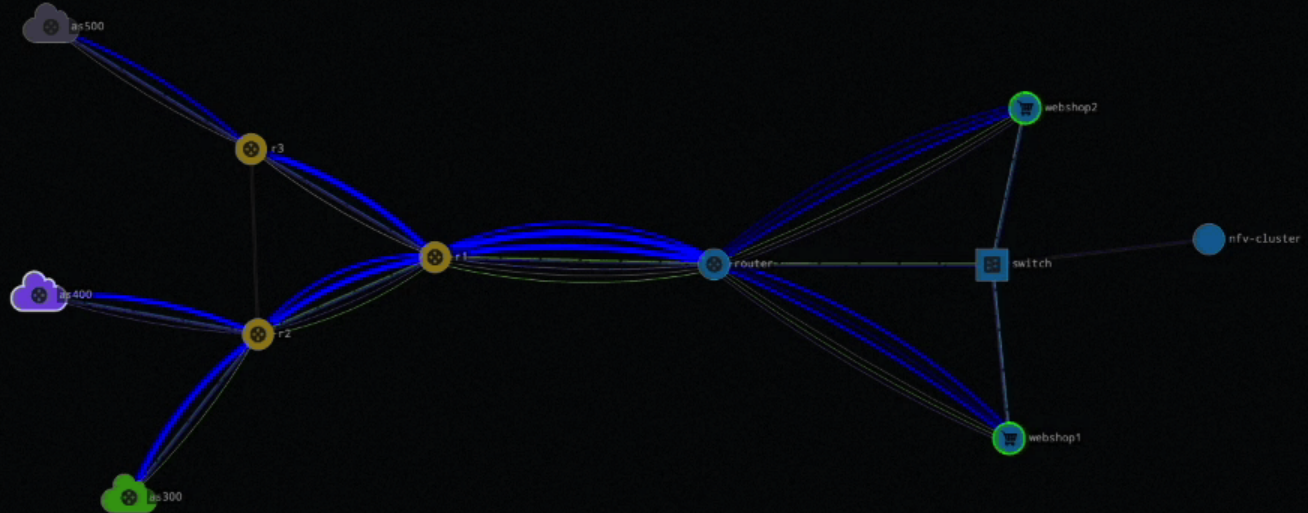
By using SDN and containerized NFV, the SARNET agent can resolve network and application level attacks.

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: e2.edge2.as400

CPU utilization Password attack

Normal operation

Object information

e2.edge2.as400

```
KIND: router
COMPUTE#DISKIMAGE: 1e81f761-db3b-4e3b-8ae3-2b4f60da0185#img-router
COMPUTE#SPECIFICCE: exogeni#XOSmall
IC2#WORKERNodeID: uva-nl-w1
REQUEST#HASRESERVAT...: request#Active
REQUEST#INDOMAIN: uvanlmsite.rdf#uvanlmsite/Domain/vm
CPU#PCT: 22
```



SC16 DEMO SARNET Operational Level

sarnet

Connected

SARNET demo

Control loop delay:



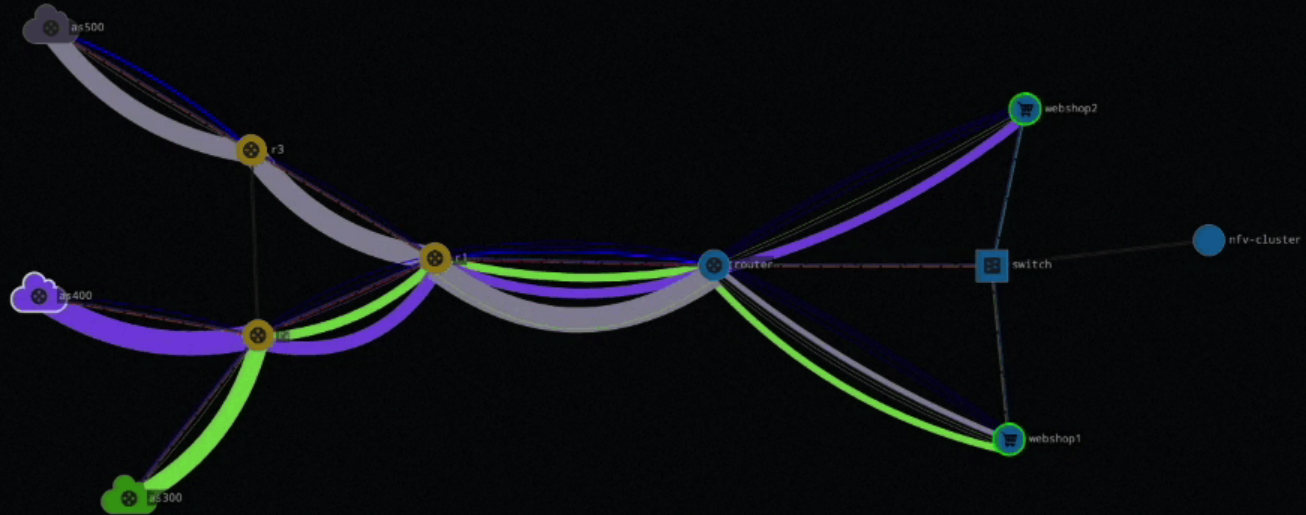
By using SDN and containerized NFV, the SARNET agent can resolve network and application level attacks.

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: e2.edge2.as400

CPU utilization Password attack

Normal operation

Object information

e2.edge2.as400

```
KIND: router
COMPUTE#DISKIMAGE: 1e81f761-db3b-4e3b-8ae3-2b4f60da0185#img-router
COMPUTE#SPECIFIC: exogeni#XOSmall
IC2#WORKERNODEID: uva-nl-w1
REQUEST#HASRESERVAT...: request#Active
REQUEST#INDOMAIN: uvanlvm/site.rdf#uvanlvm/site/Domain/vm
CPU#PCT: 17
```

Edge domains flood the network with UDP traffic



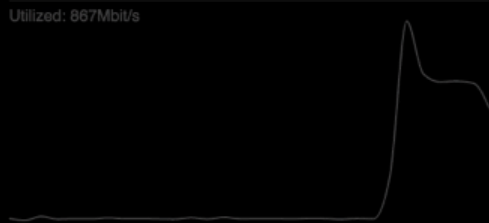
SC16 DEMO SARNET Operational Level

Secure Autonomous Response Network SARNET agent metrics

Network metrics

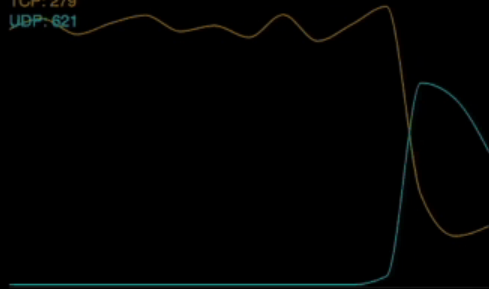
Bandwidth:

Utilized: 867Mbit/s



Flows:

TCP: 279
UDP: 621



Application metrics

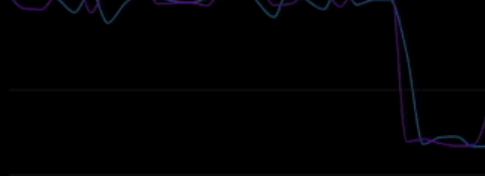
CPU:

Webshop 1: 38%
Webshop 2: 60%



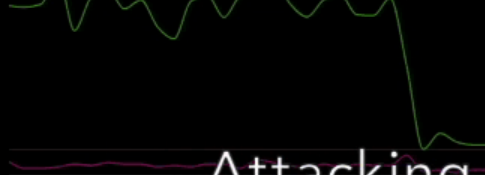
Successful transactions:

Webshop 1: 39
Webshop 2: 99

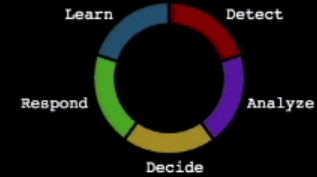


Login attempts:

Successful: 24
Failed: 2



Control loop



DETECT

Revenue below threshold
Abnormal UDP flows detected

ANALYZE

DDoS domains: AS300, AS400, AS500

DECIDE

Filter UDP traffic at edge domains

RESPOND

Attacking domains are identified

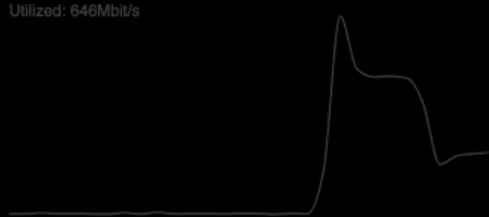
SC16 DEMO SARNET Operational Level

Secure Autonomous Response Network SARNET agent metrics

Network metrics

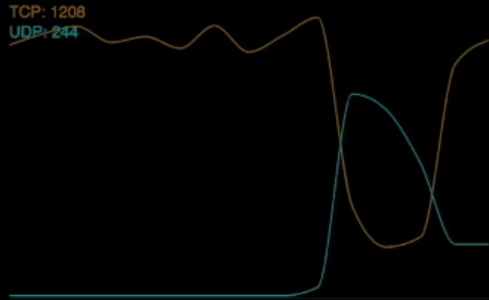
Bandwidth:

Utilized: 646Mbit/s



Flows:

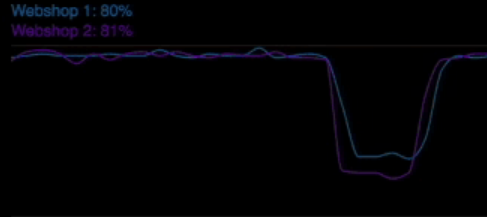
TCP: 1208
UDP: 244



Application metrics

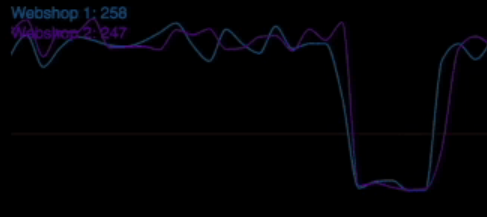
CPU:

Webshop 1: 80%
Webshop 2: 81%



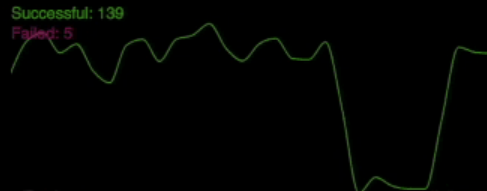
Successful transactions:

Webshop 1: 258
Webshop 2: 247

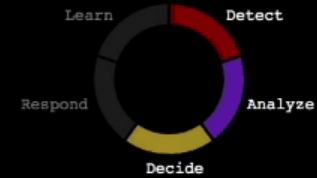


Login attempts:

Successful: 139
Failed: 5



Control loop



DETECT

Abnormal UDP flows detected

ANALYZE

DDoS domains: AS300, AS400, AS500

DECIDE

Filter UDP traffic at edge domains

RESPOND

Flow filters are installed at the network edge

SC16 DEMO SARNET Operational Level

sarnet

Connected

SARNET demo

Control loop delay:



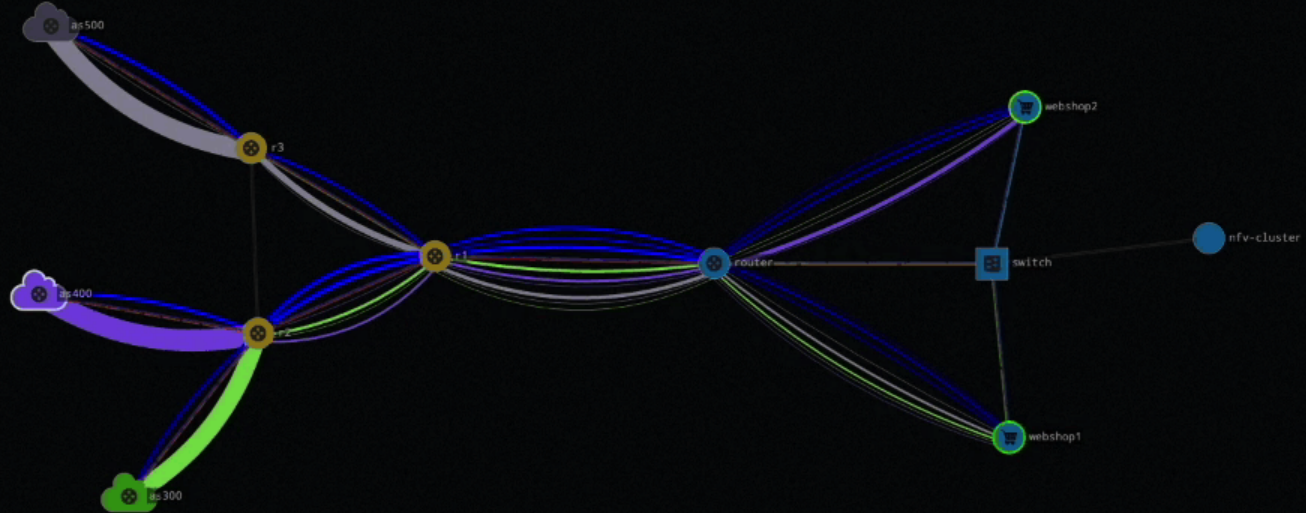
By using SDN and containerized NFV, the SARNET agent can resolve network and application level attacks.

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: e2.edge2.as400

CPU utilization Password attack

Normal operation

Object information

e2.edge2.as400

```
KIND: router
COMPUTE#DISKIMAGE: 1e81f761-db3b-4e3b-8ae3-2b4f60da0185#img-router
COMPUTE#SPECIFIC:CE: exogeni#XOSmall
IC2#WORKERNodeID: uva-nl-w1
REQUEST#HASRESERVAT...: request#Active
REQUEST#INDOMAIN: uvanlvm/site.rdf#uvanlvm/site/Domain/vm
CPU#PCT: 27
```

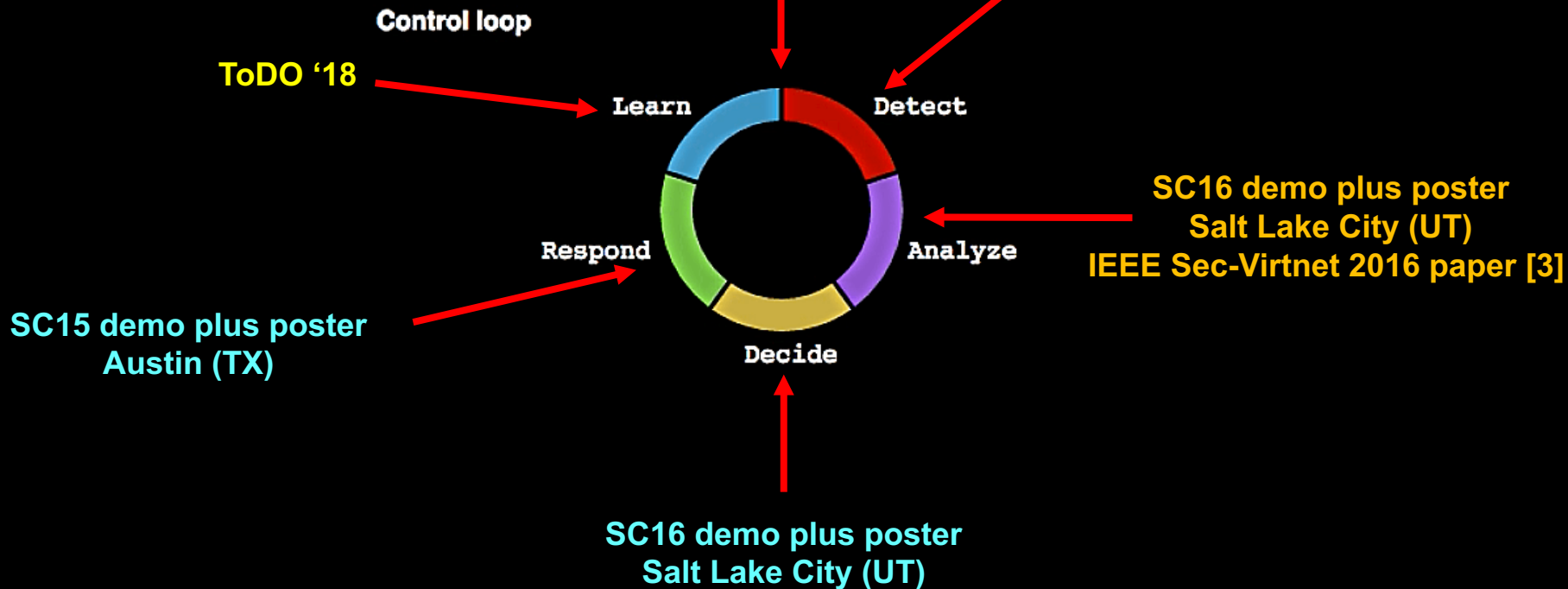
Service is restored



Status SARNET Operational Level

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

CoreFlow
Berkeley Internship 2016
SC16 INDIS workshop paper [2]



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.

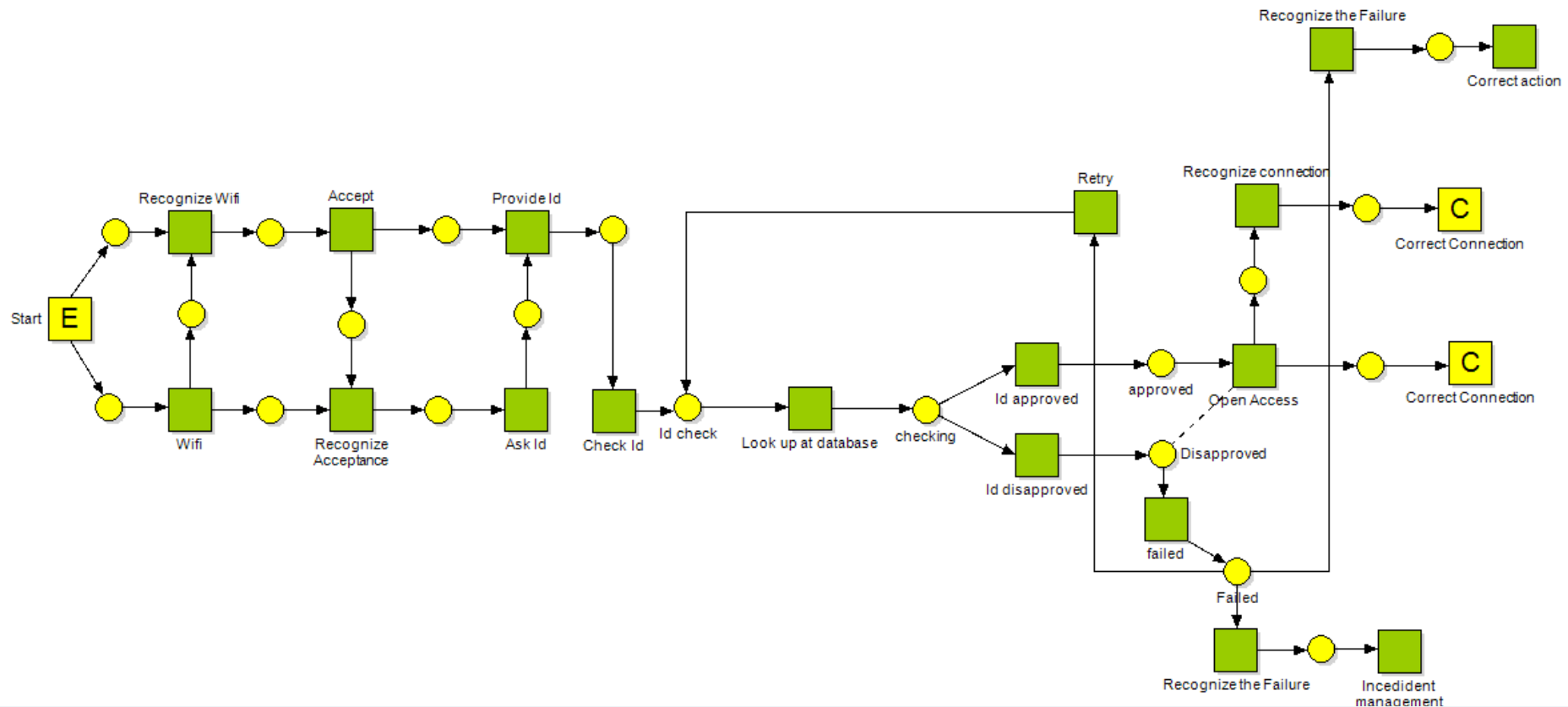
Agent Based Modelling Framework

	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:

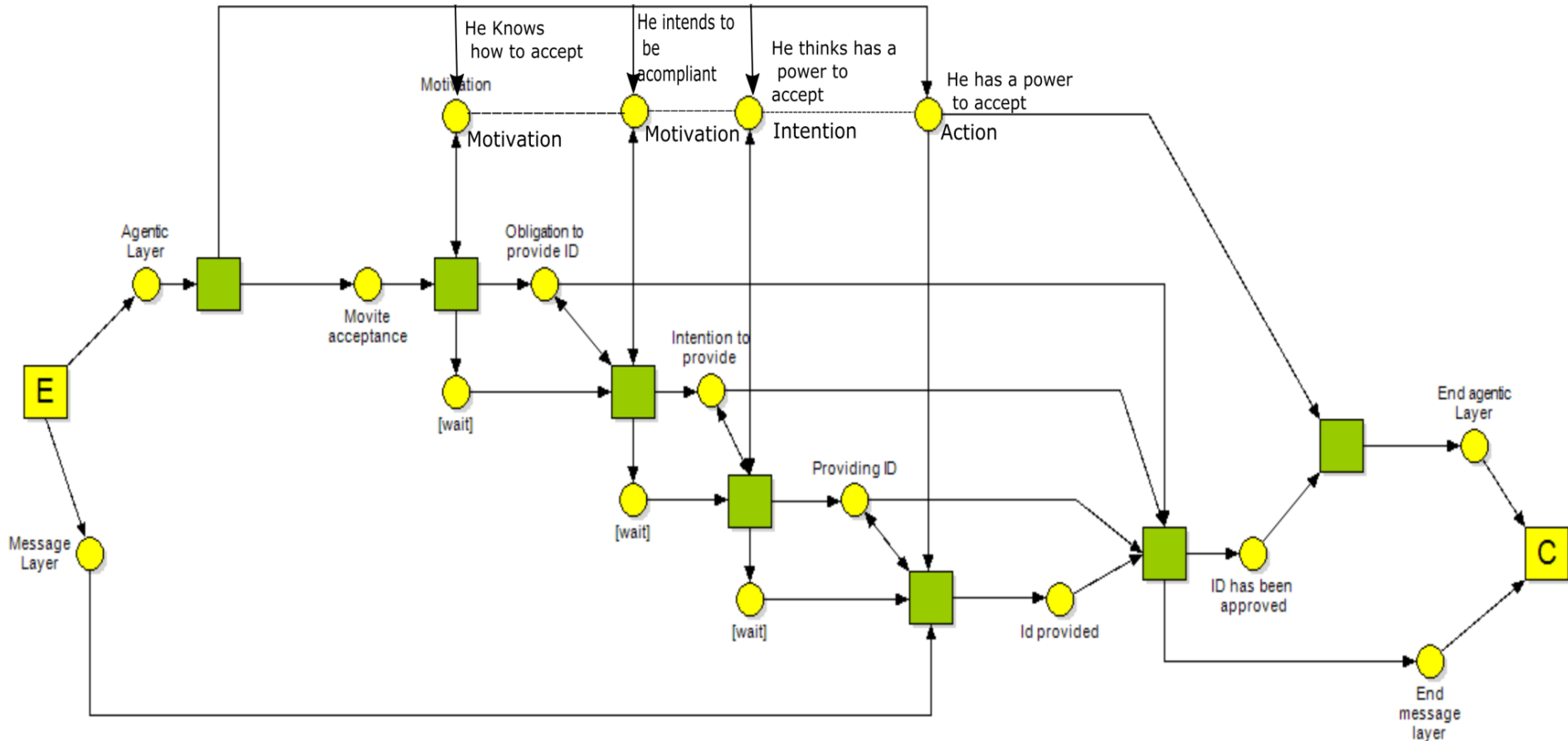
- the signal layer— describes **acts**, side-effects and failures showing outcomes of actions in a topology.
- the action layer—**actions**: performances that bring a certain result,
- the intentional layer—**intentions**: commitments to actions, or to build up intentions,
- the motivational layer—**motives**: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

Simplified Eduroam case at signalling layer



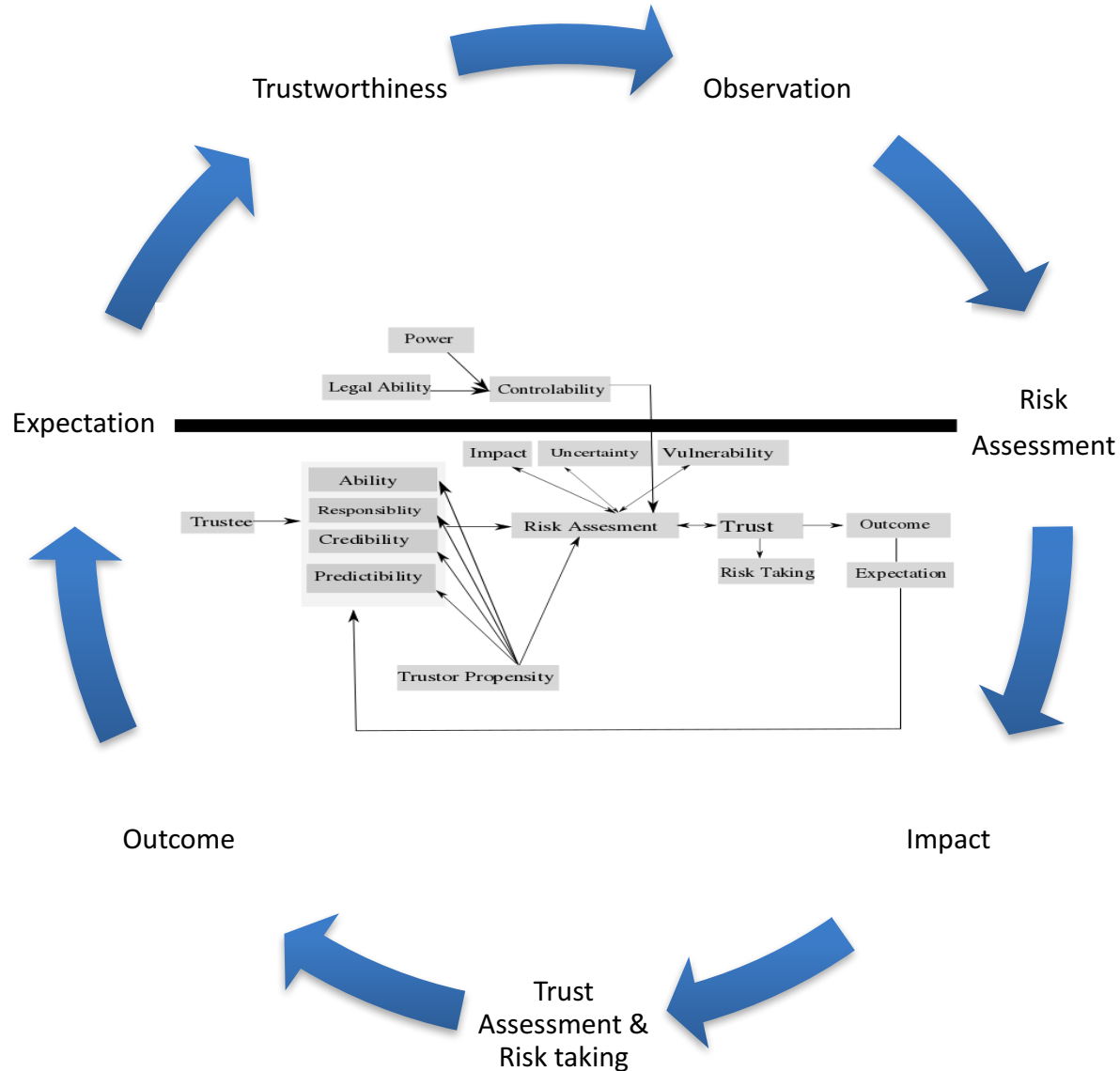
Petri net of EduRoam Case
(first step)

Describing Intentions, Motivations and Actions

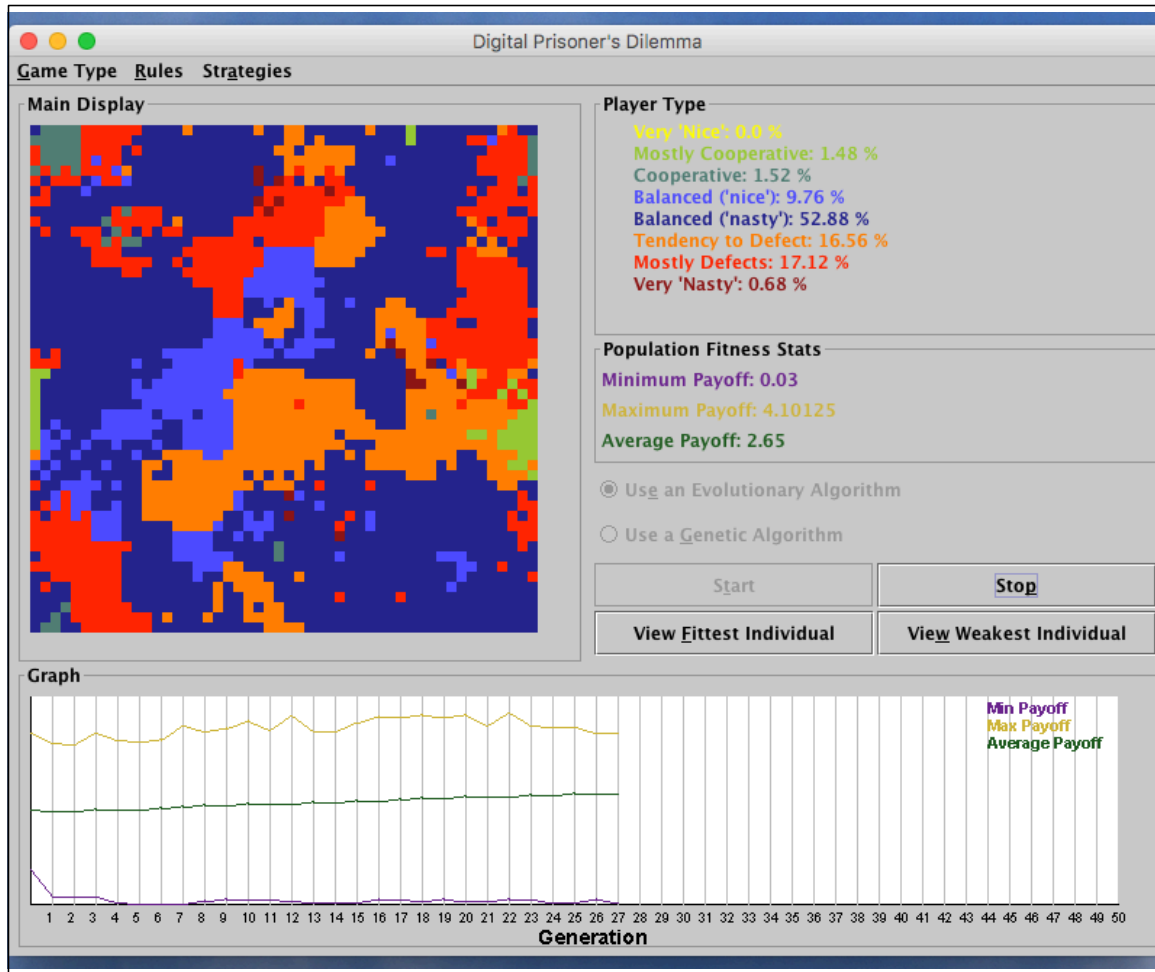


Petri net of EduRoam Case

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.

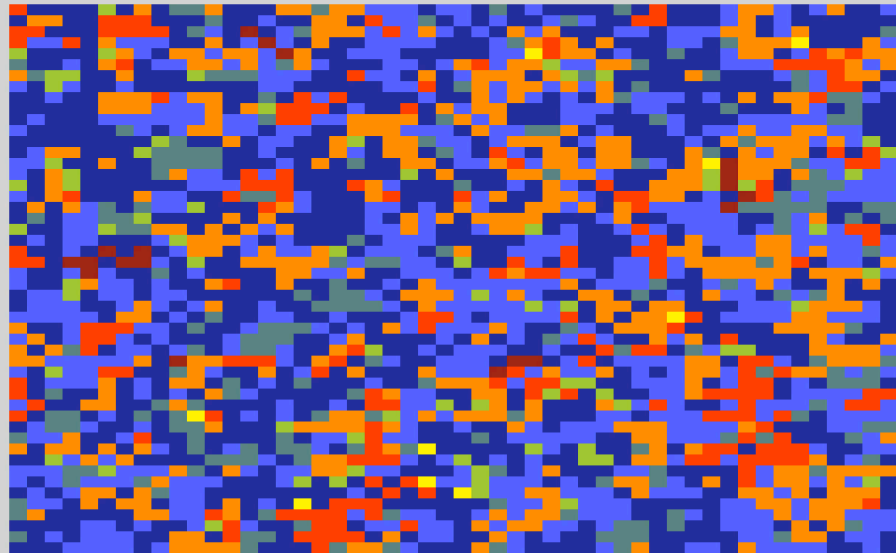
This type of simulation will be base to simulate more complex collaborations of autonomous organizations.

ABM Simulation

Evolutionary Prisoner's Dilemma

Game Type Rules Strategies

Main Display



Player Type

Very 'Nice': 0.36 %
Mostly Cooperative: 2.88 %
Cooperative: 8.44 %
Balanced ('nice'): 27.16 %
Balanced ('nasty'): 34.88 %
Tendency to Defect: 17.8 %
Mostly Defects: 7.72 %
Very 'Nasty': 0.76 %

Population Fitness Stats

Minimum Payoff: 0.1925

Maximum Payoff: 4.105

Average Payoff: 2.24

Use an Evolutionary Algorithm

Use a Genetic Algorithm

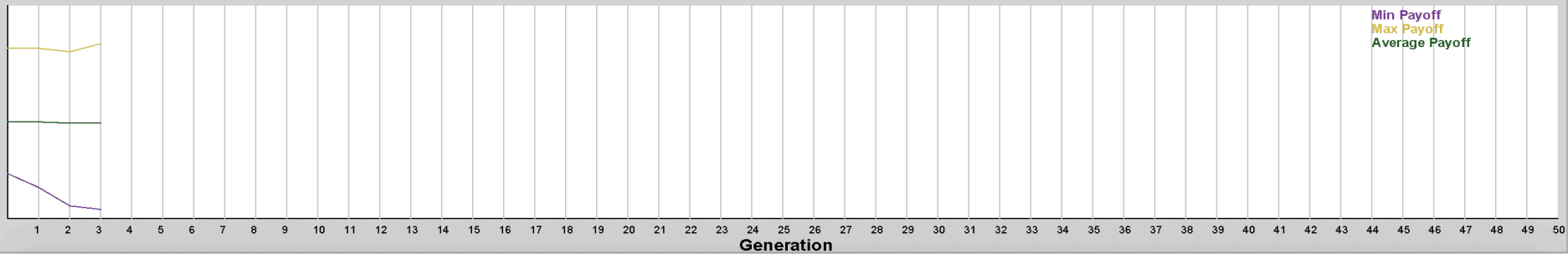
Start

Stop

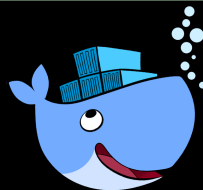
View Fittest Individual

View Weakest Individual

Graph



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

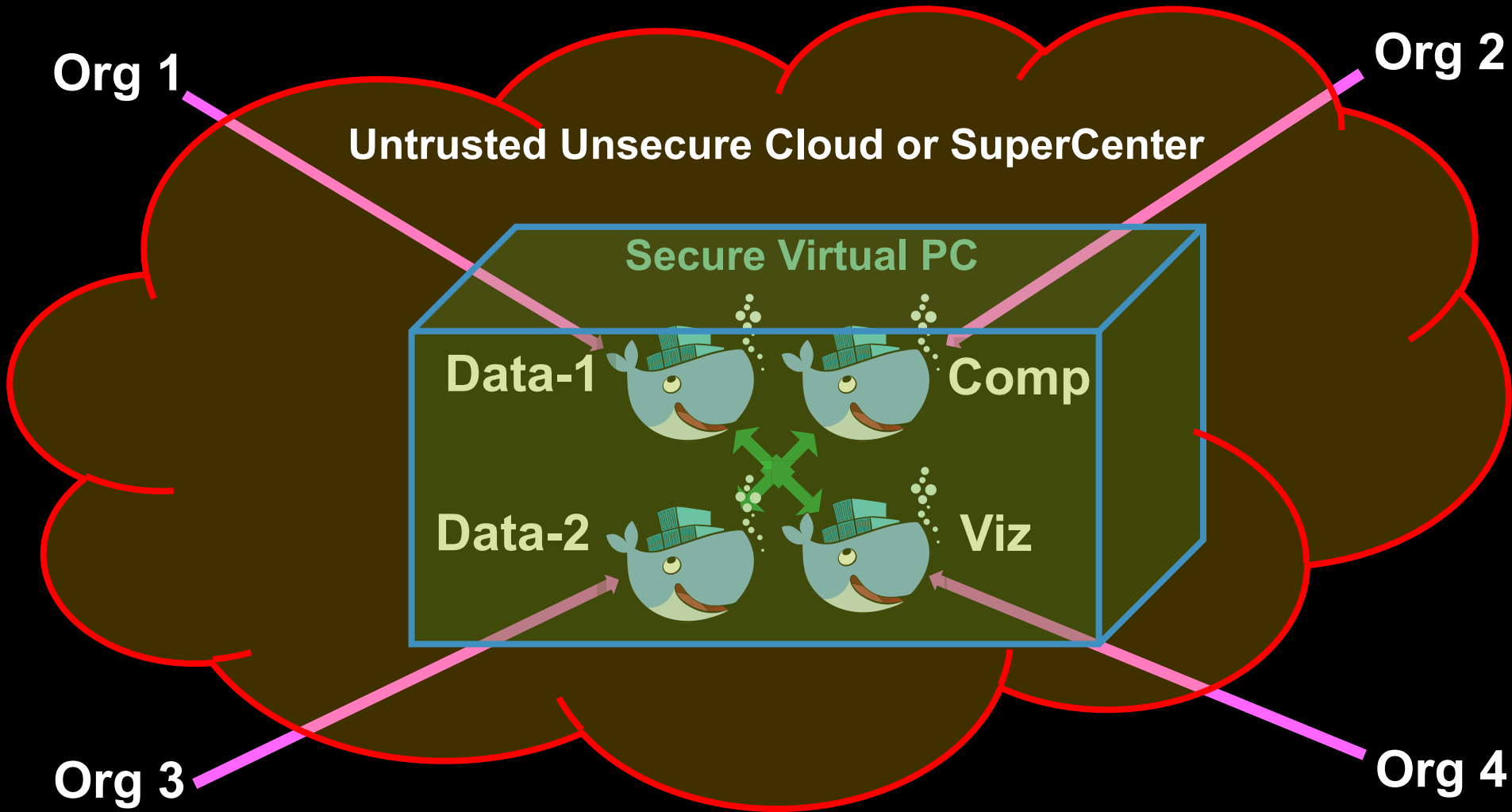
Comp

Data-2

Viz

Org 3

Org 4



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

