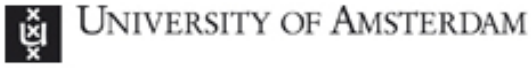
Creating a SARNET and a Sarnet Alliance

using the Ciena/GENI testbed Research projects

November 16-19th 2015

Austin Texas



Ameneh Deljoo: a.deljoo@uva.nl, Ralph Koning: r.koning@uva.nl, Ben de Graaff: b.degraaff@uva.nl
Leon Gommans: leon.gommans@klm.com ,Tom van Engers: t.m.engers@uva.nl,
Cees de Laat: delaat@uva.nl

Cyber Security readiness

Creating a SARNET Alliance
Sharing intelligence and defensive power
Booth #2321 of SURF

SARNET
Security state / defense tactics automation

SARNET
Topology dynamics

SARNET Alliance research

Why: **Understand the value of collaboration** between alliance members in terms of **risk reduction** increasing trust**, cost benefit and revenue impact.**

What: Provide **a-priori insight** into the **rationale of creating an alliance**.

How: Use the **Service Provider Group Framework*** to institutionalize **trust** by arranging common **rules**, its **execution** (administration & enforcement) and **judgement**.

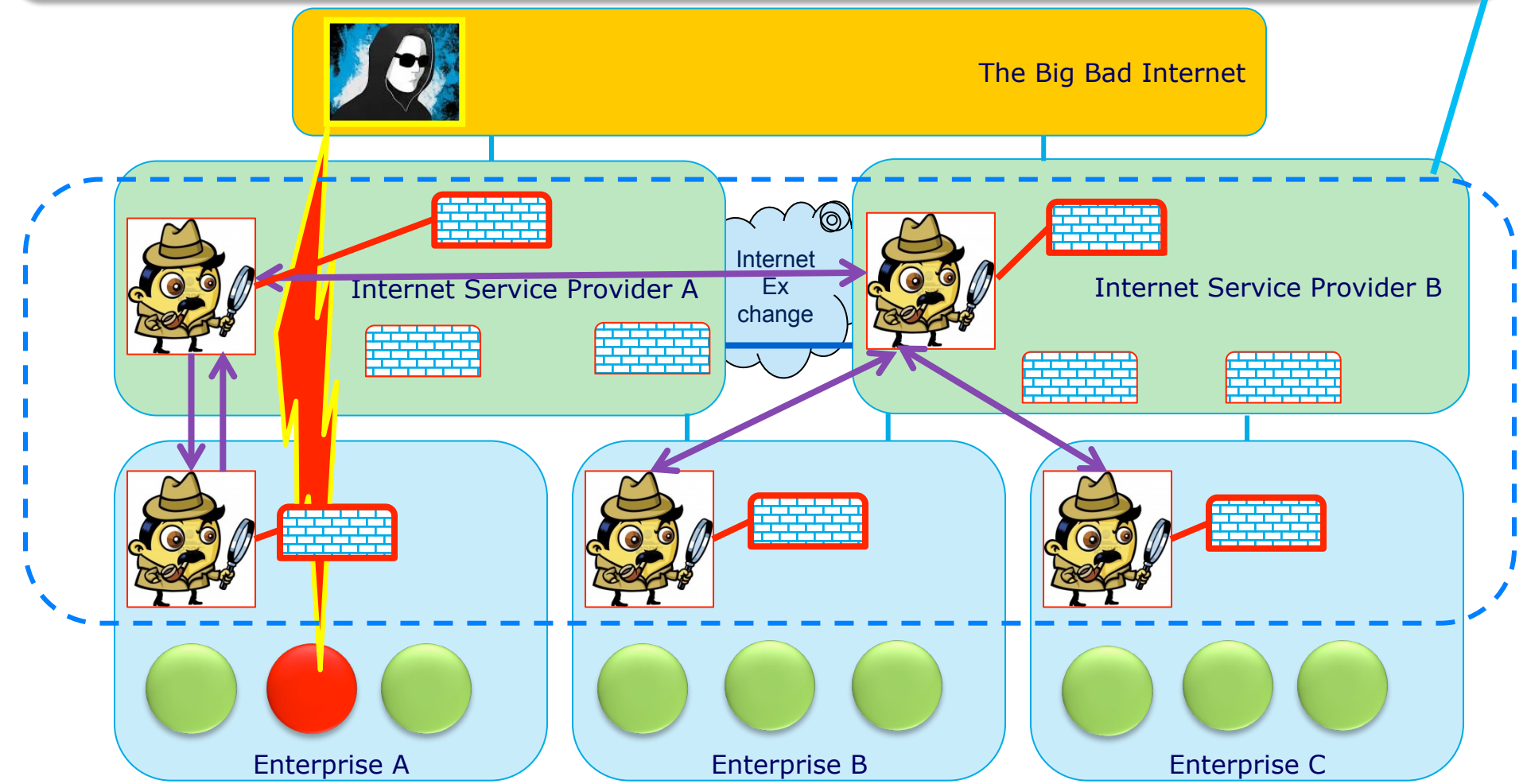
With what: A distributed computational model of an alliance that analyses the **policies** each autonomous member constructs from the common set of **rules**.

Result: The models can become base of an **Information Security Management System** that establishes, reviews, maintains and improves information security amongst alliance members.

* Leon Gommans, John Vollbrecht, Betty Gommans-de Bruiijn, Cees de Laat, **The Service Provider Group framework A framework for arranging trust and power to facilitate authorization of network services,** Future Generation Computer Systems 45 (2015) pg 176–192

SARNET Alliance concept

SARNET Alliance research using Service Provider Group concept



SARNET Research

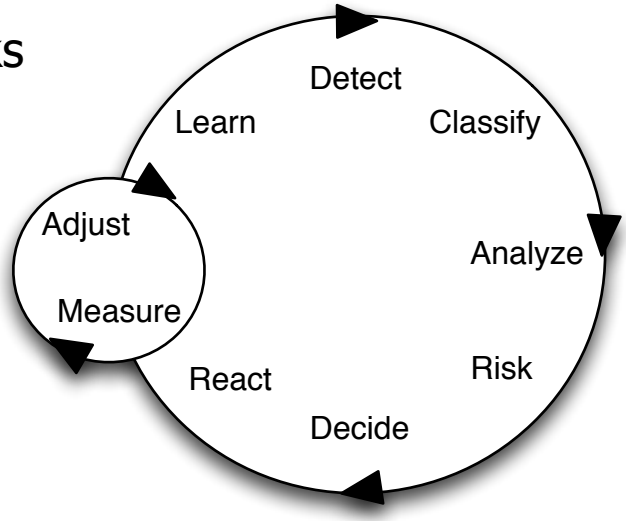
Testbed provided by ciena using geni technology

SARNET

Why: **Automatically reduce impact** of cyber attacks on revenue.

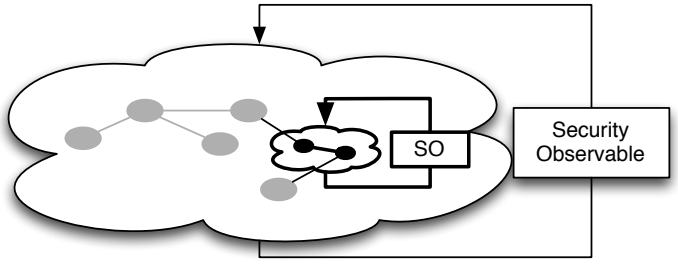
What: Create **highly reactive** networks that **autonomously** defend against cyber attacks.

How: Using control loops that **monitor** the security state, **evaluate** attack impact and effectiveness of defense strategies, whilst **learning** to apply **best possible defense**.



SARNET control loop

With what: **Software Defined Networks** and **Network Function Virtualization** can be used to converge the network to a new state that is **more resilient** to the attack.



SARNET with security observable

Result: Attacks no longer impact critical infrastructure, and infrastructure **responds** more **rapidly** to new **attacks** of the same kind.

Interactive DDoS Analysis