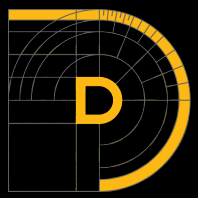


The **DETER** Project

The DETER Project:
Experimentation Facilities and Tools for Security Researchers

Alefiya Hussain
hussain@isi.edu

The DETER Project

- Testbed facility:
  - Publicly available national resource to
    - support a broad base of users and experiments
    - increase scope and scale
- Research program:
  - Advance tools and methodologies for
    - multiple levels of fidelity
    - extract and maintain knowledge
- Education and Community building:
  - Foster collaborative science through research leverage and sharing of knowledge

The Testbed Facility

- Started in 2003, Emulab-based platform, funded by NSF and DHS
- ~550 PC-based nodes
  - Berkeley, CA - ~200 Nodes
  - Los Angeles, CA - 330 Nodes
  - Arlington, VA – 20 Nodes
  - High bandwidth interconnects
- **Cyber security focused** experiment isolation, tools and technologies, risky experiments

Design

Scenario Composition

Goal: Manage scale and complexity in cyber security experiments

Design Constraints / Invariants

Scenario Specification

Reposit

Execute

DETERLab

Approach: Tools and methodologies to make it approachable

Containers

Monitor/ Logging

Challenges: Manage for sensibility and feasibility if experiments

A

Animate

Graphs

Mining

Analyze

Research Programs

- Advanced Testbed Technologies

  O(500) → O(100,000)

  http://containers.deterlab.net

- Experiment Control and Monitoring

  nodes → agents

  http://montage.deterlab.net

- Large scale Data Analysis

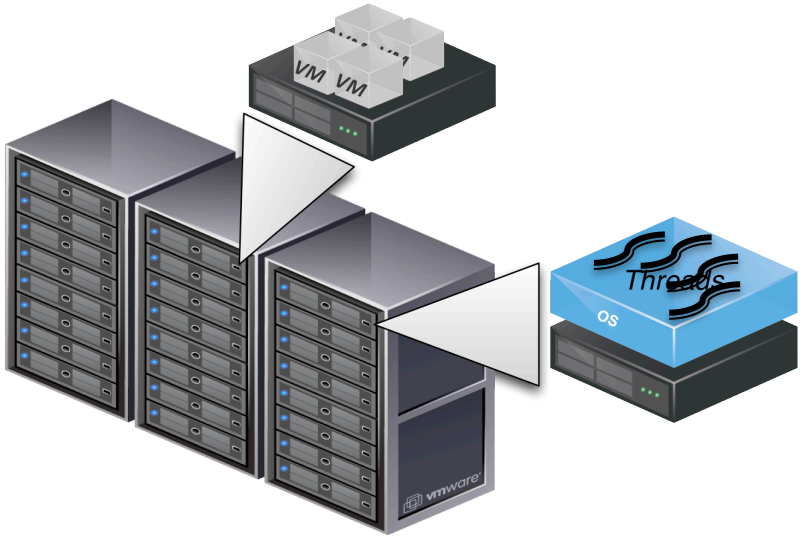
  data → understanding

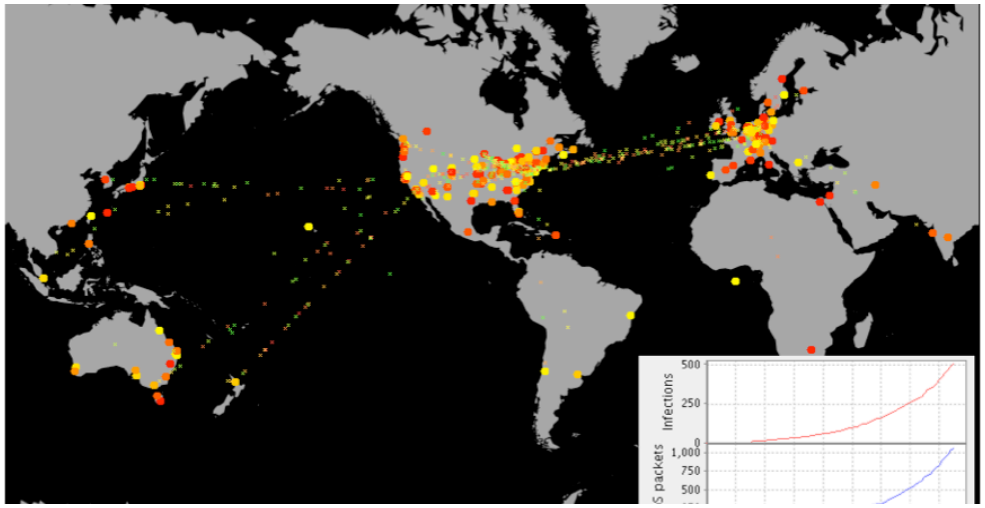
  http://thirdeye.deterlab.net

Testbed Technologies

O(500) ⟶ O(100,000)

http://containers.isi.deterlab.net

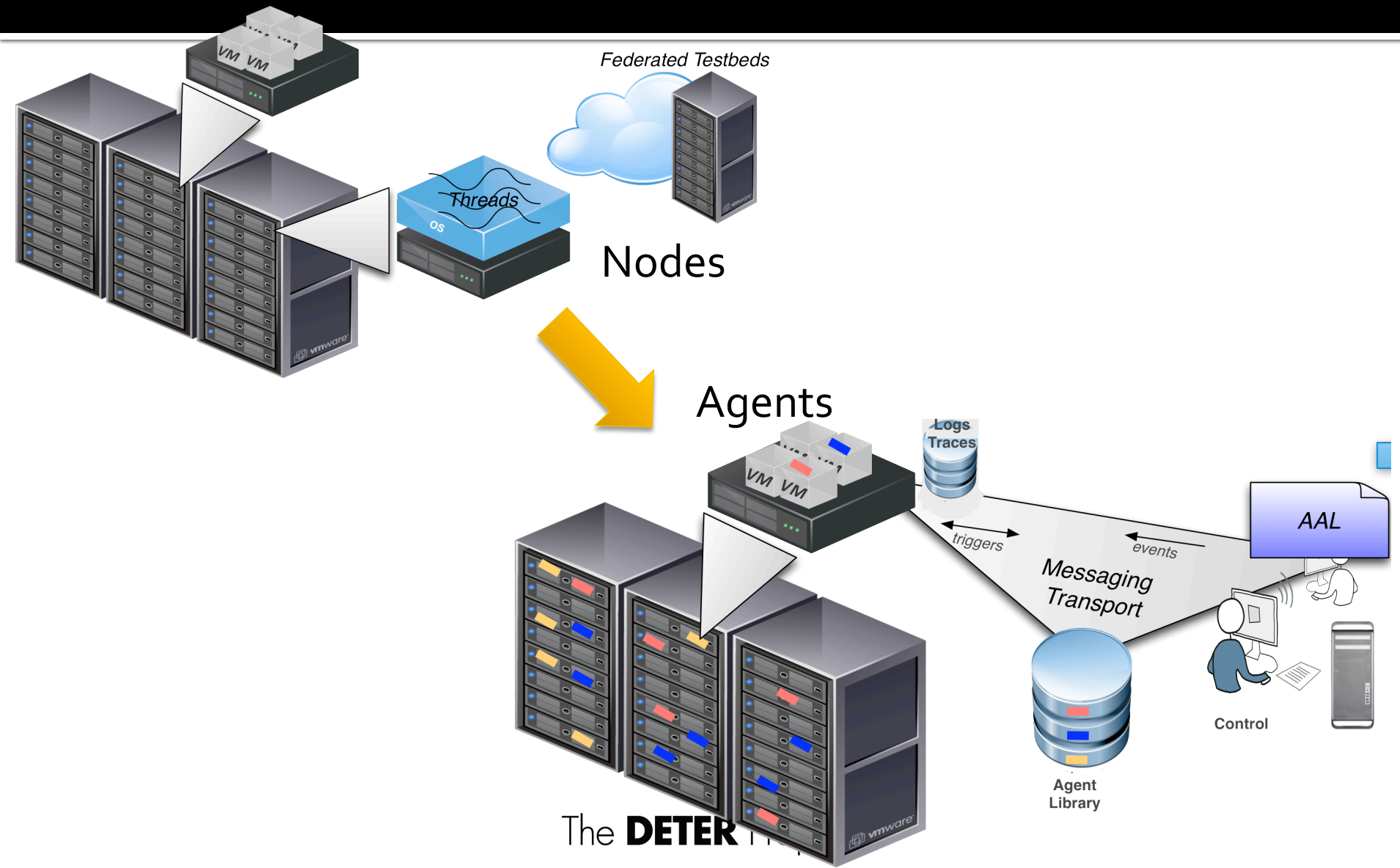




100K host, worm,botnet, ddos attack

http://www.deter-project.net

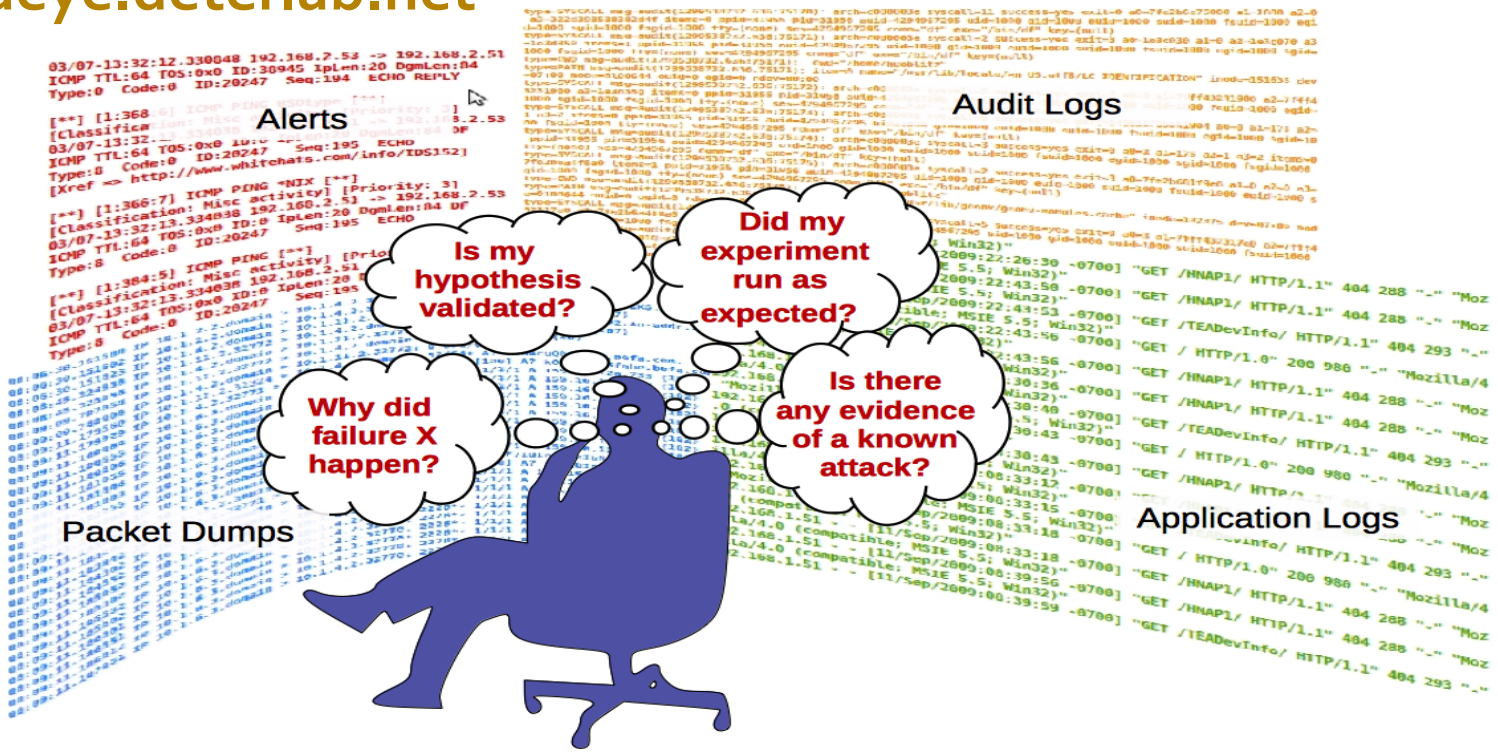
Experiment Control & Monitoring



Large Scale Data Analysis

- data ⟶ understanding

http://thirdeye.deterlab.net



Viswanathan, Husssain, Mirkovic, Schwab, Wroclawski
A Semantic Framework for Data Analysis in Networked Systems,
USENIX NSDI 2011

The **DETER** Project

Research Programs

- Advanced Testbed Technologies

  O(500) → O(100,000)

  http://containers.deterlab.net

- Experiment Control and Monitoring

  nodes → agents

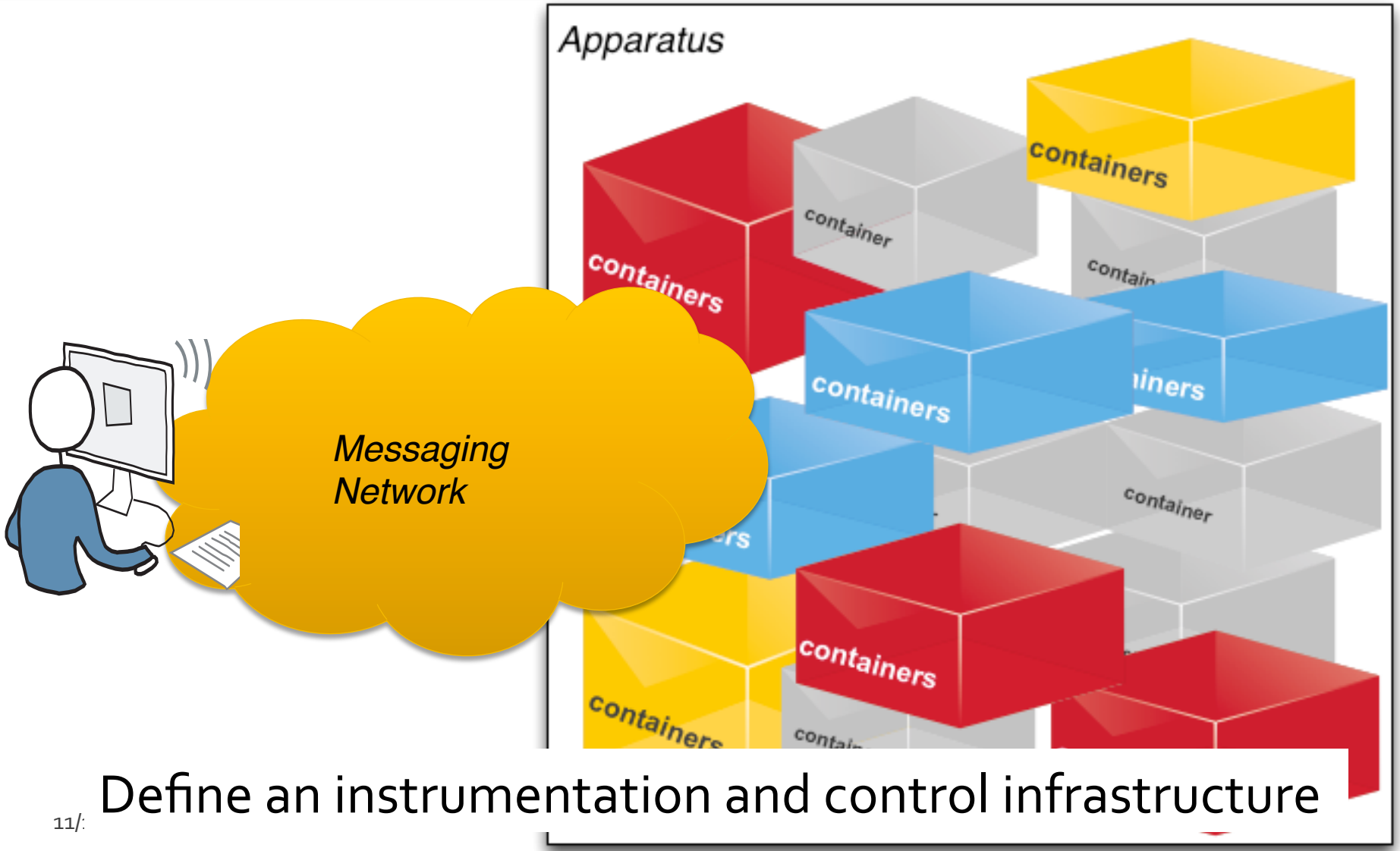
  http://montage.deterlab.net

- Large scale Data Analysis

  data → understanding

  http://thirdeye.deterlab.net

Frame of Reference



Define an instrumentation and control infrastructure

Performance at Scale

- O(500) → O(100,000) containers
- Event Frequency
  - 100K host * 10 events/sec = 1M messages/sec
- Event Bandwidth
  - 4KB/message = 4GB/sec

Previous solutions did not scale

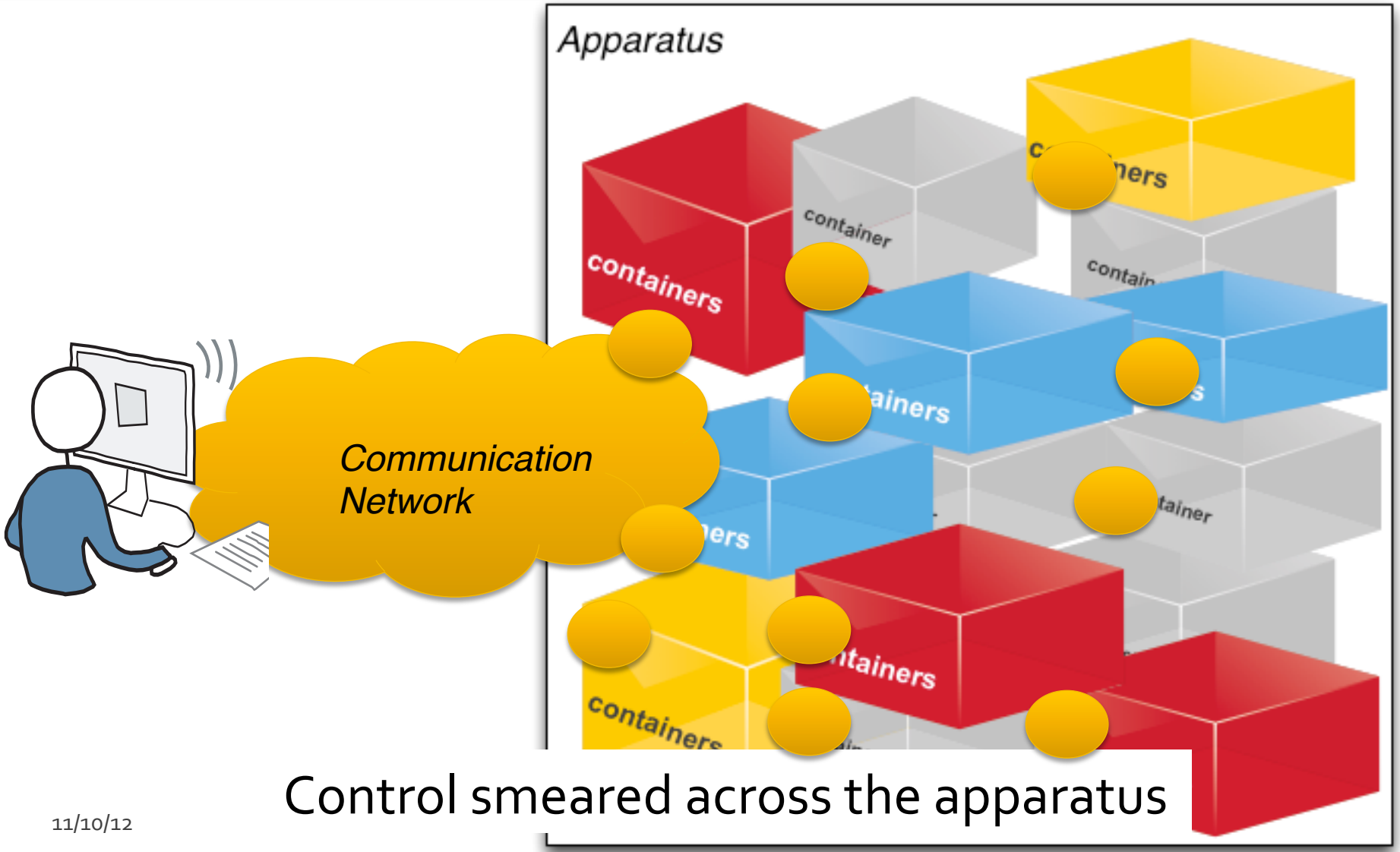
Controlling the Apparatus

- O(500) control technologies
  - tevc event system
  - SEER

- O(100,000) control technologies
  - *Montage AGent Infrastructure* (MAGI)

Two decisions for the infrastructure

Scalable Communication



Control smeared across the apparatus

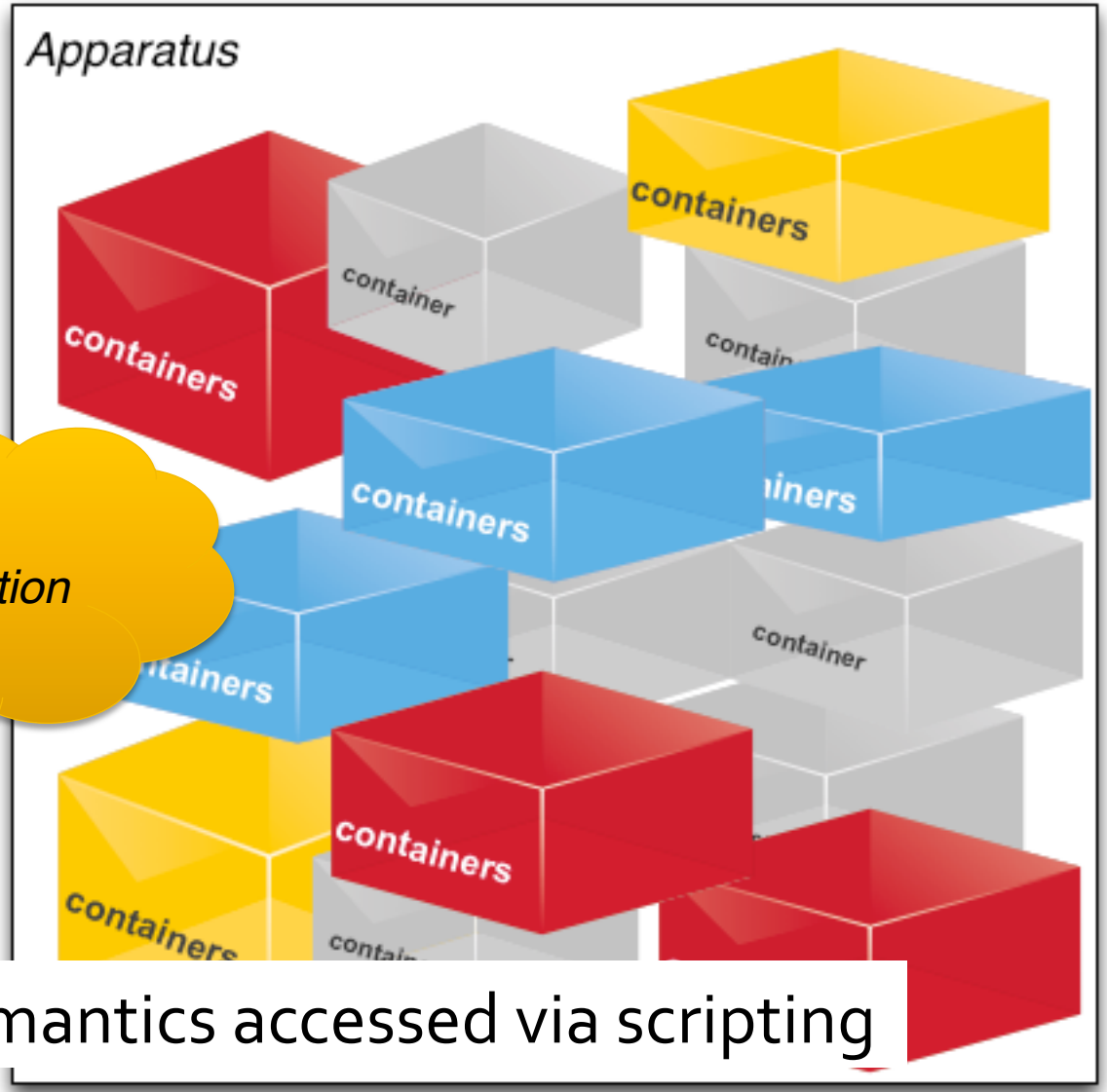
Control Specification

Graphical frontends

Programming Languages

Scripting

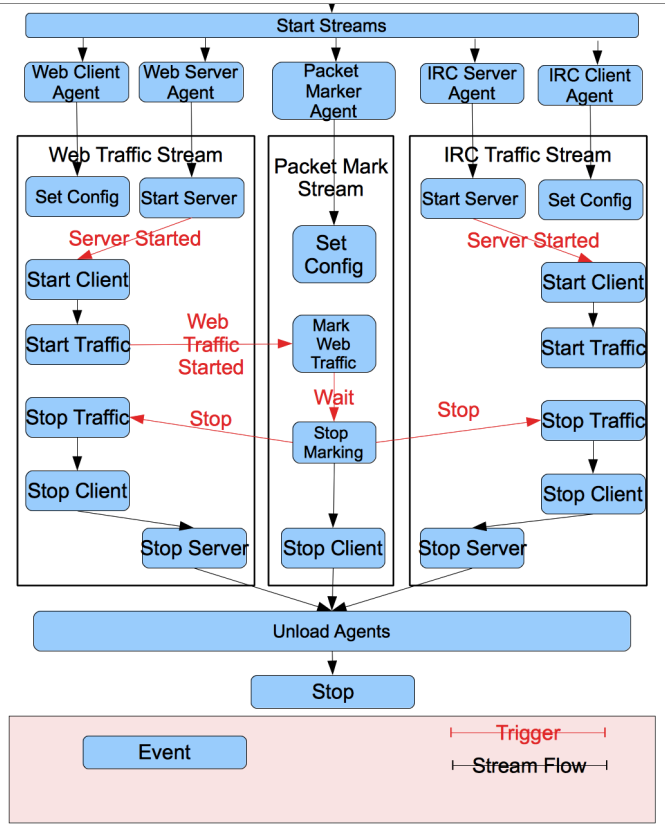
Communication Network



Control semantics accessed via scripting

MAGI: Current Status

- Control Semantics
  - time based and event based triggers
  - workflows
- 25+ agents and growing
  - traffic, monitoring
- Users and contributors
  - SAFER community
  - Education



Past, Present, Future

- Research facility for cyber security R&D
- Proactive Research programs to address the needs of experimental cyber security
- Growing Community
  - DARPA, DHS, NSF, Industry, Education

Thank you

- Join DETER

http://www.deter-project.org

Alefiya Hussain
hussain@isi.edu