Rethinking Cyber R&D for Compromised Environments

Jim Brase

Deputy Program Director Intelligence
Lawrence Livermore National Laboratory

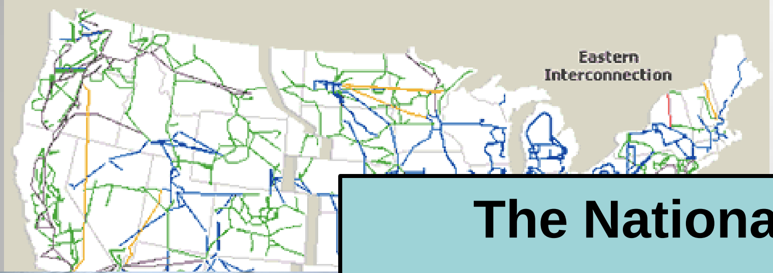
Secretary of Energy
Advisory Board

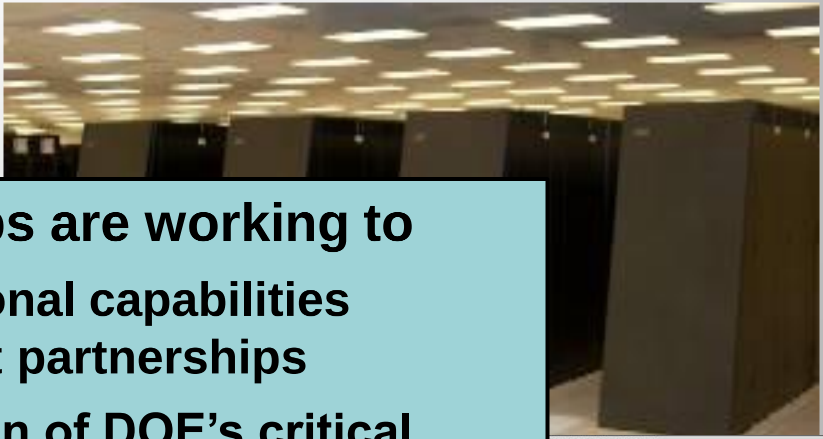
October 12, 2011

LLNL-PRES-505151

This work was performed under the auspices of the U.S. Department of Energy
by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

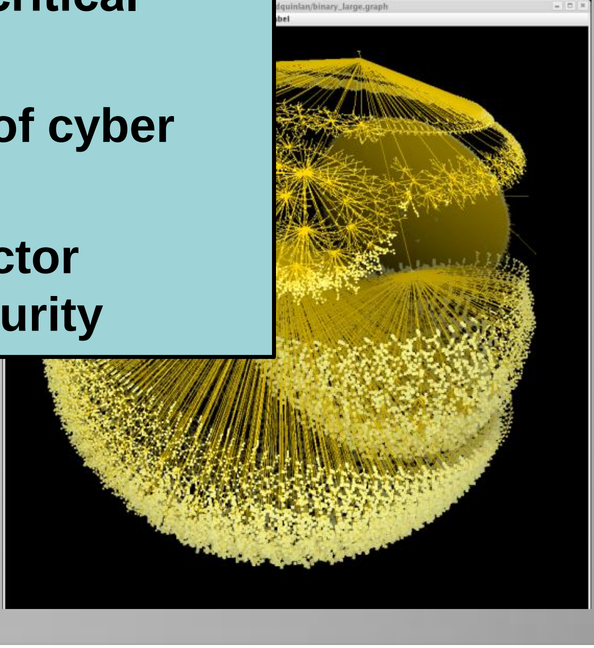
Cyber has emerged as one of today's most critical national security domains





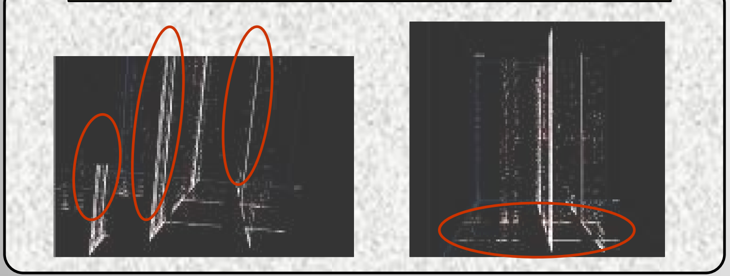
The National Labs are working to

1. **Strengthen our national capabilities through government partnerships**
2. **Ensure the protection of DOE's critical information**
3. **Build the scientific foundations of cyber and network science**
4. **Help to establish new private sector partnerships for sustainable security**

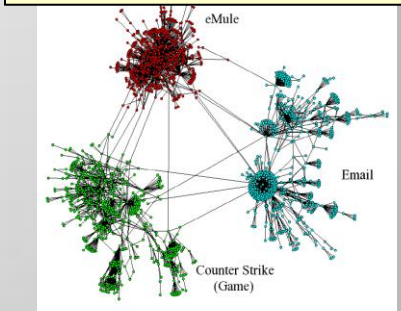


LLNL’s cyber R&D builds on DOE’s long-term investment in computing and information science

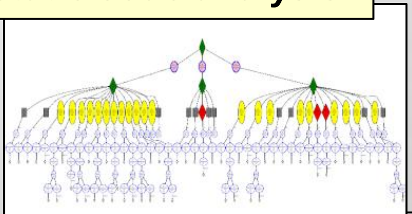
Cybersecurity incident analysis

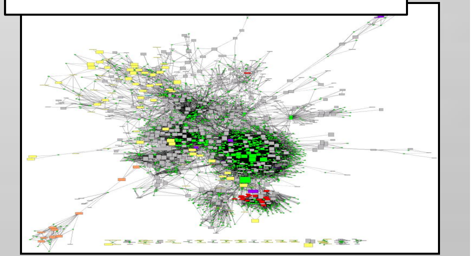


Machine learning in complex systems

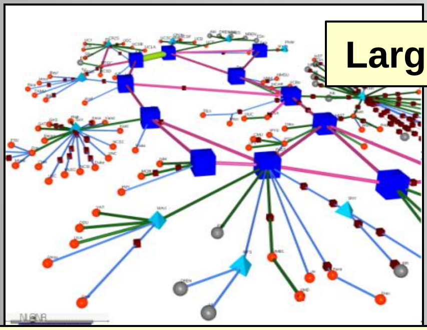


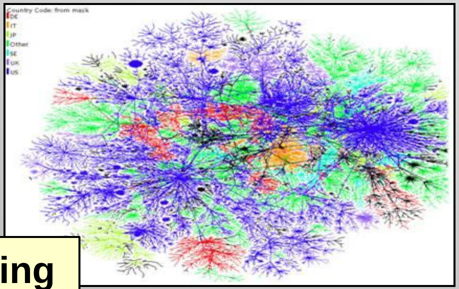
Parallel methods for static code analysis



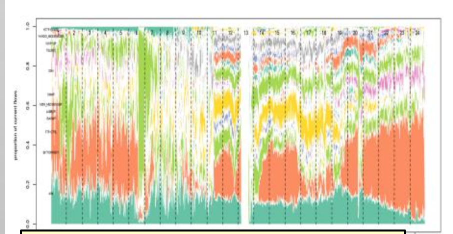


Large-scale semantic graphs





Computer network mapping

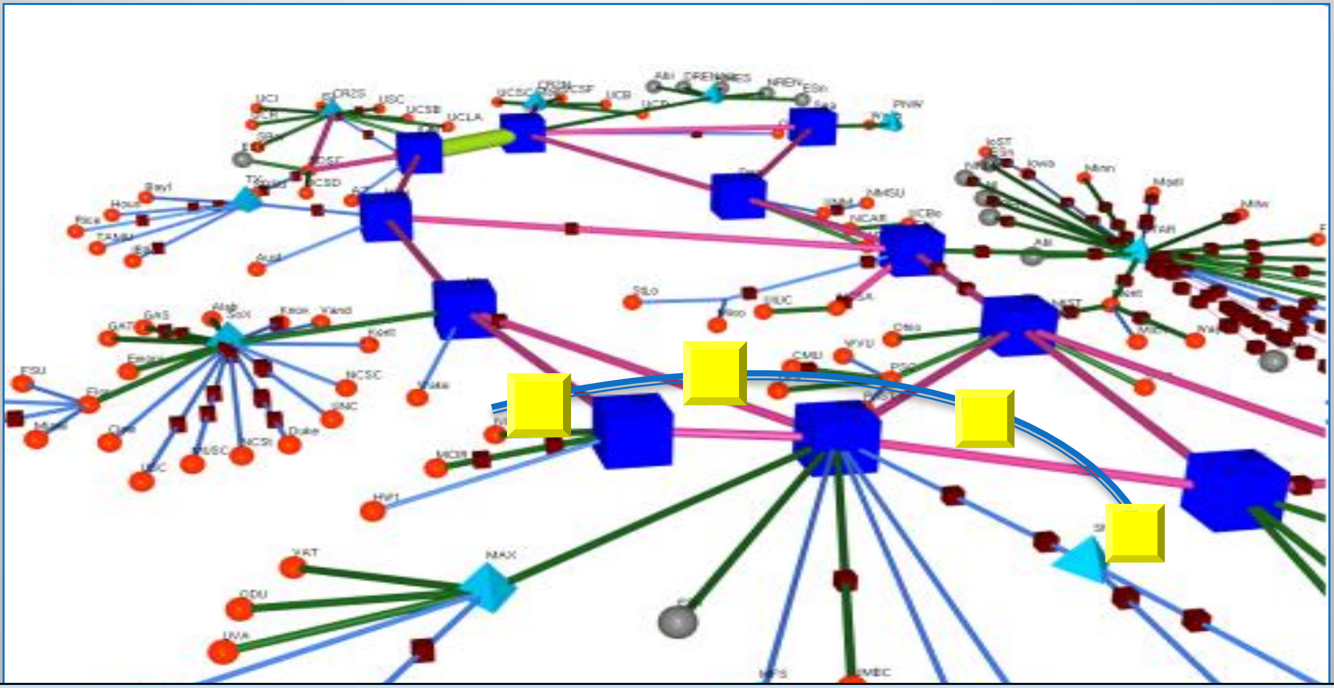


Behavioral models of network activity

DOE’s LDRD program has been a key contributor to developing new concepts

1997 2003 2010

Today's approach to cybersecurity is not sustainable



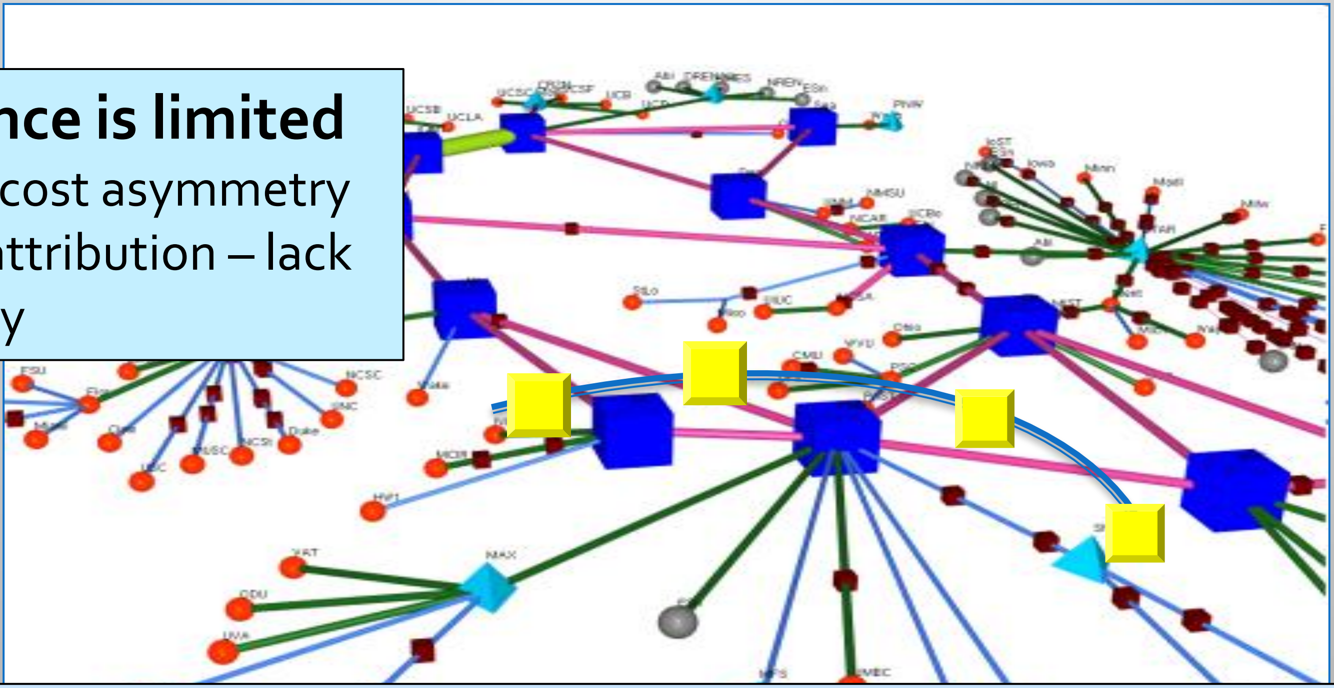
The rapidly evolving Information network environment

- No such thing as a perimeter – mobility and cloud – your network is everywhere
- Convergence and proliferation increase attack paths
- Growing adversary capabilities – polymorphism, persistence, …

Deterrence and protection should be important elements of a security strategy

Deterrence is limited

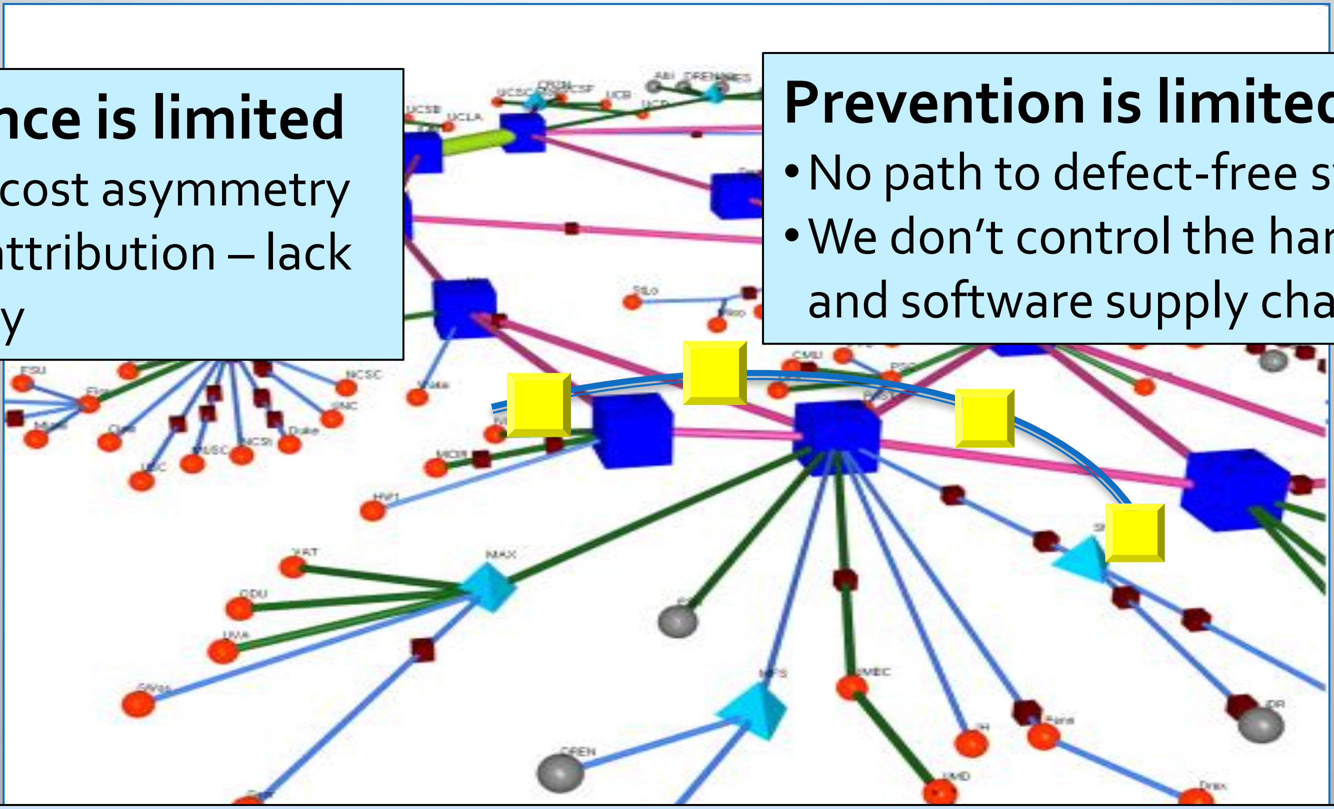
- Growing cost asymmetry
- Limited attribution – lack of identity



The rapidly evolving Information network environment

- No such thing as a perimeter – mobility and cloud – your network is everywhere
- Convergence and proliferation increase attack paths
- Growing adversary capabilities – polymorphism, persistence, …

Deterrence and protection should be important elements of a security strategy



Deterrence is limited

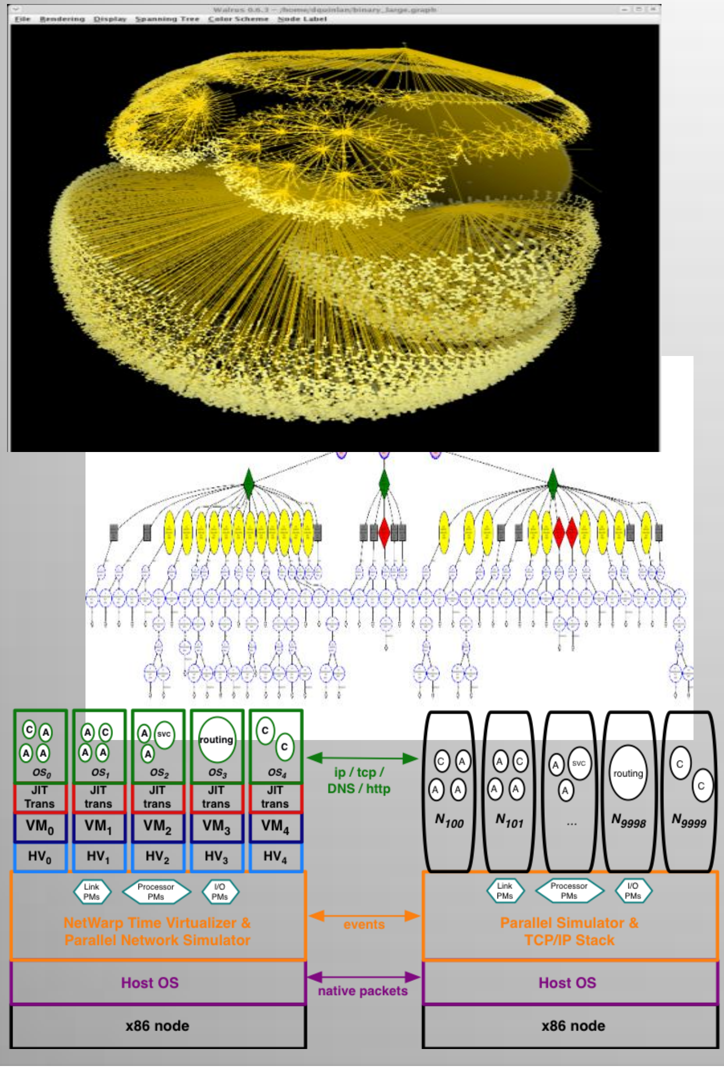
- Growing cost asymmetry
- Limited attribution – lack of identity

Prevention is limited

- No path to defect-free systems
- We don’t control the hardware and software supply chains

Capable adversaries are and will be in our systems and networks

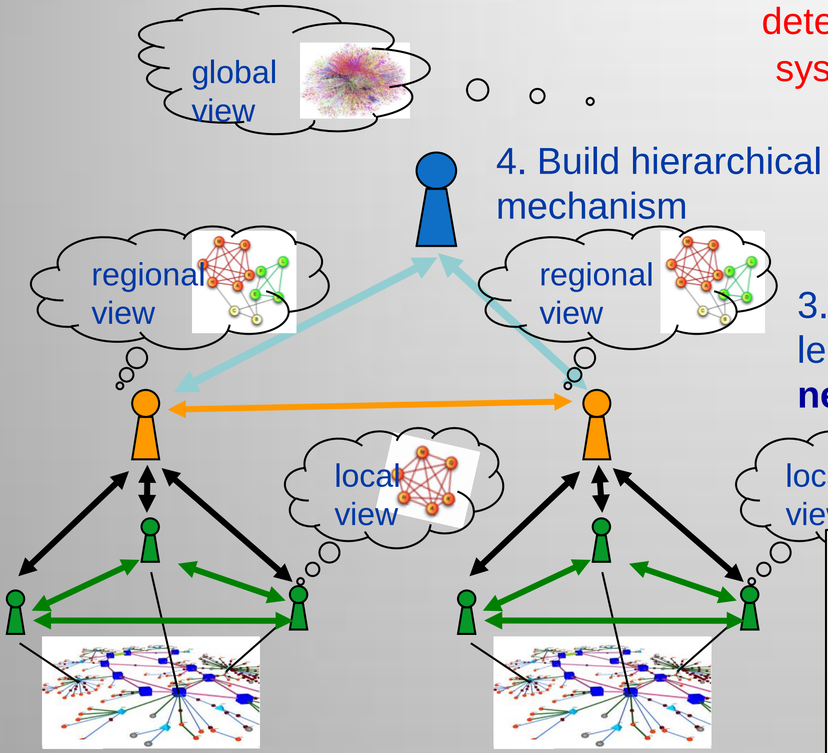
Change the goal – don’t protect networks, protect critical missions


Walrus 0.6.3 – /home/dquinlan/binary_large.graph
File Rendering Display Spanning Tree Color Scheme Node Label
C A A A
A C A A
A svc A
routing
C C
OS_0 OS_1 OS_2 OS_3 OS_4
JIT Trans
JIT trans
VM_0 VM_1 VM_2 VM_3 VM_4
HV_0 HV_1 HV_2 HV_3 HV_4
ip / tcp / DNS / http
N_{100} N_{101} ... N_{9998} N_{9999}
Link PMs
Processor PMs
I/O PMs
NetWarp Time Virtualizer & Parallel Network Simulator
events
Parallel Simulator & TCP/IP Stack
Host OS
native packets
x86 node

To do this we need new capabilities

- Situational awareness – Know the network and its activities at full-scale and in real-time
- Predict network behaviors - how the mission will interact with the network and how defensive activities will affect it
- Adapt protection and response for the specific activity, environment, and threat

Situational Awareness - From signatures to network behaviors



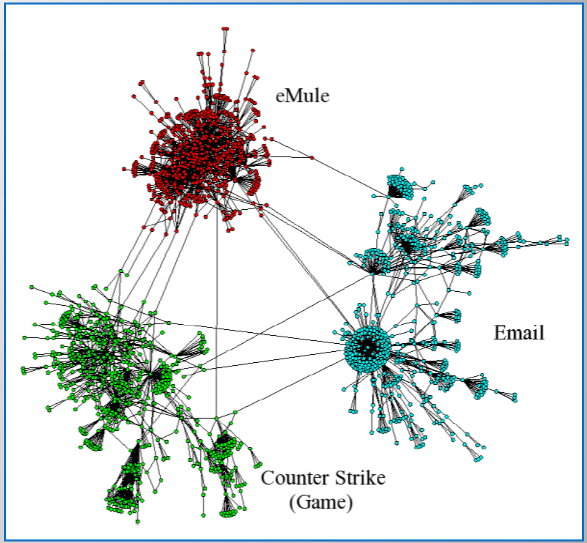
Anomalous activity detections (compromised system, suspicious IPs)

4. Build hierarchical control mechanism

3. Develop machine learning **algorithms for network behavior**

2. Build a local **graph representation** of activity

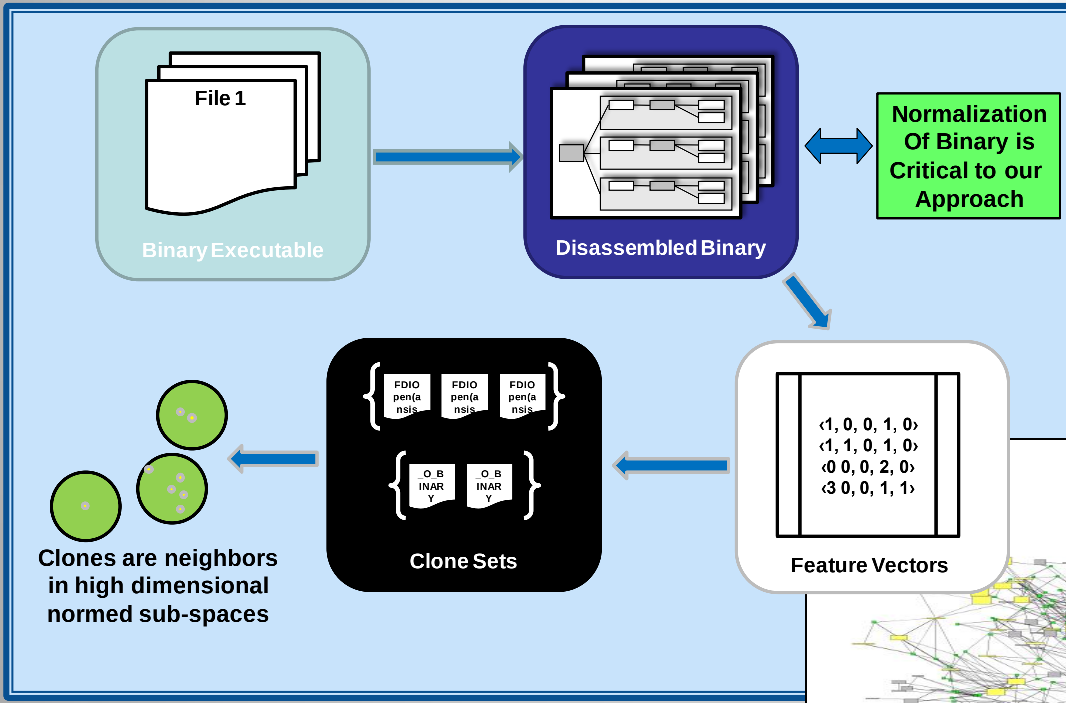
1. **Collect data** from physical networks



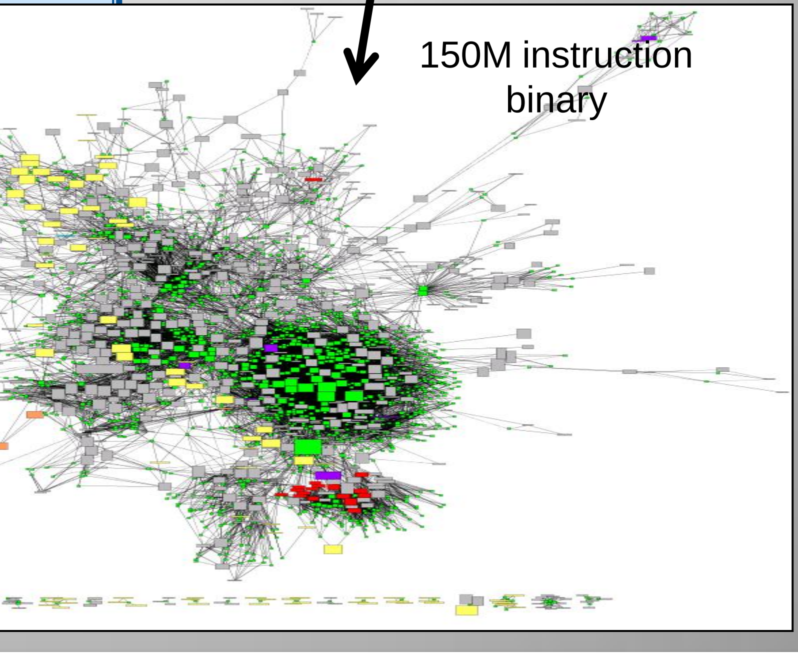
Key areas of work

- Distributed collection – not just perimeter
- Build statistical models of network behaviors represented as probabilities on graphs
- Machine learning methods to find anomalies in thousands of parallel activities
- The trade-off with user privacy

High-performance computing is enabling new approaches to real-time malware analysis



- Binary clone mapping
- Compute similarities of code segments
- Resulting graph is unique fingerprint for code
- Parallel implementation for near-real-time performance

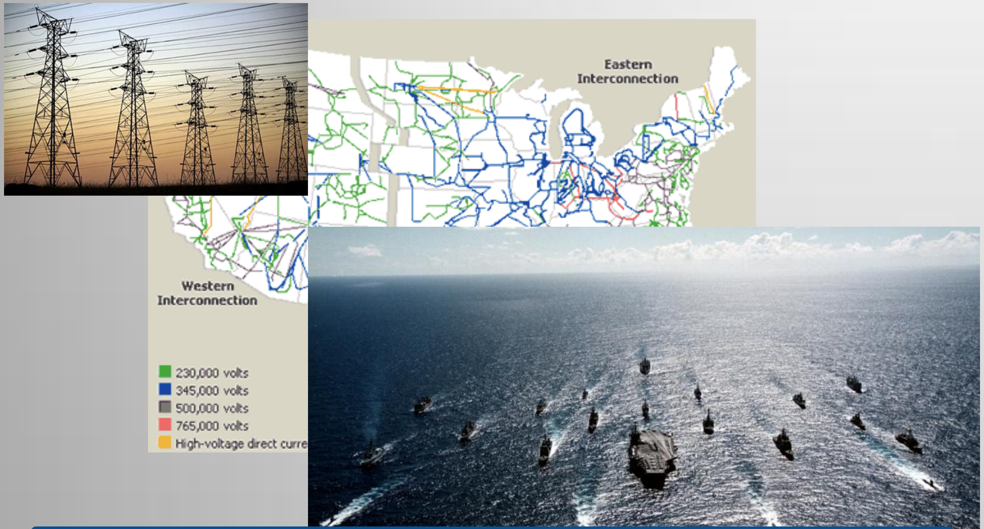


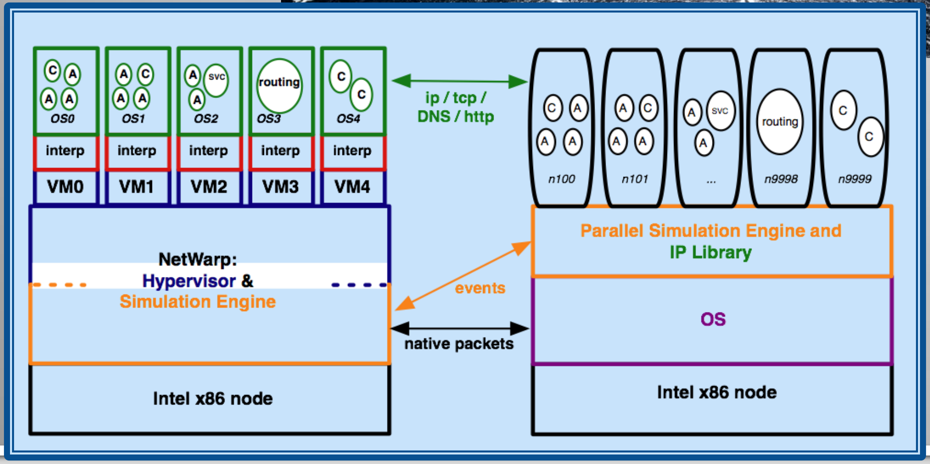
Applications to malware analysis

- Develop clone map fingerprints for large malware libraries → family trees
- Compare fingerprints of newly observed malware
- Connect to known points in family trees

The Labs are developing computational models that can predict network behaviors with fidelity and scale

Repeatable testing at scale is a major national capability gap

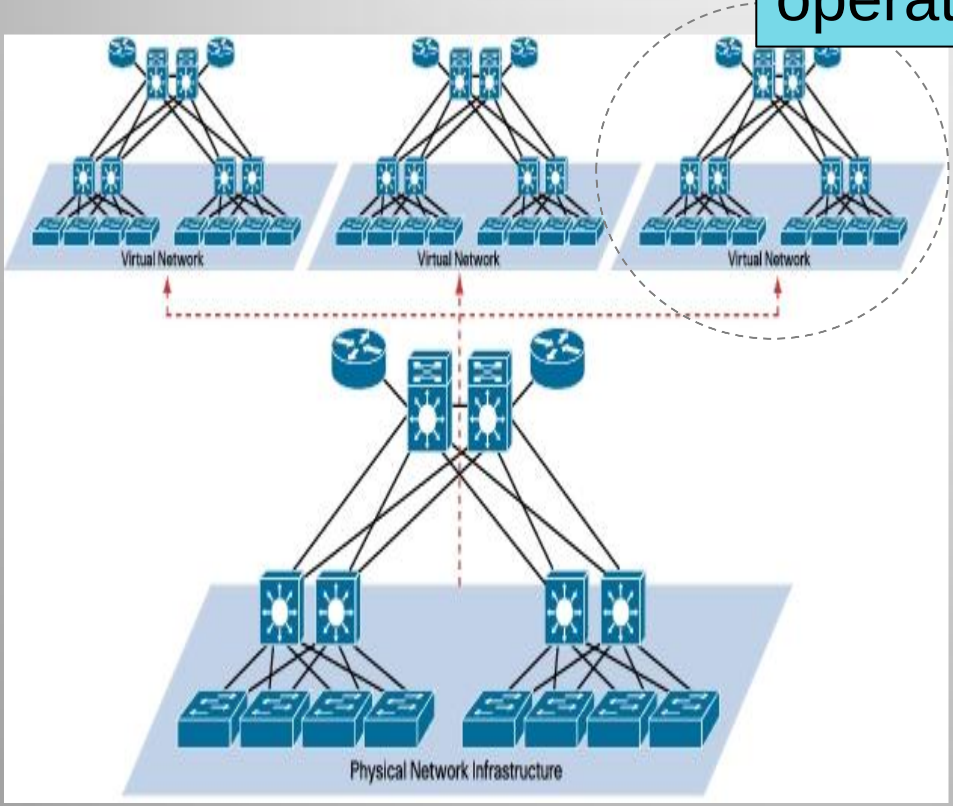




- The National Labs have long experience in simulation of complex physical systems – we need discrete dynamics on complex networks
- Ns3 – Scaling packet-level network simulations to large clusters →millions of hosts and routers
- NetWarp – Integrating virtualized networks with packet-level simulations → multiscale sim's
- Creating partnerships with government and industry for mission-focused simulation at scale

Adapting the cyber environment through dynamic mission enclaves

Change the question …. Can we keep an adversary out of our operations for a specific time?



- Create a virtual network specifically to execute a mission
- Security properties tailored to mission needs
- Needs to resist compromise only for the life of the mission

In the long-term, our strategies must integrate technology and policy approaches

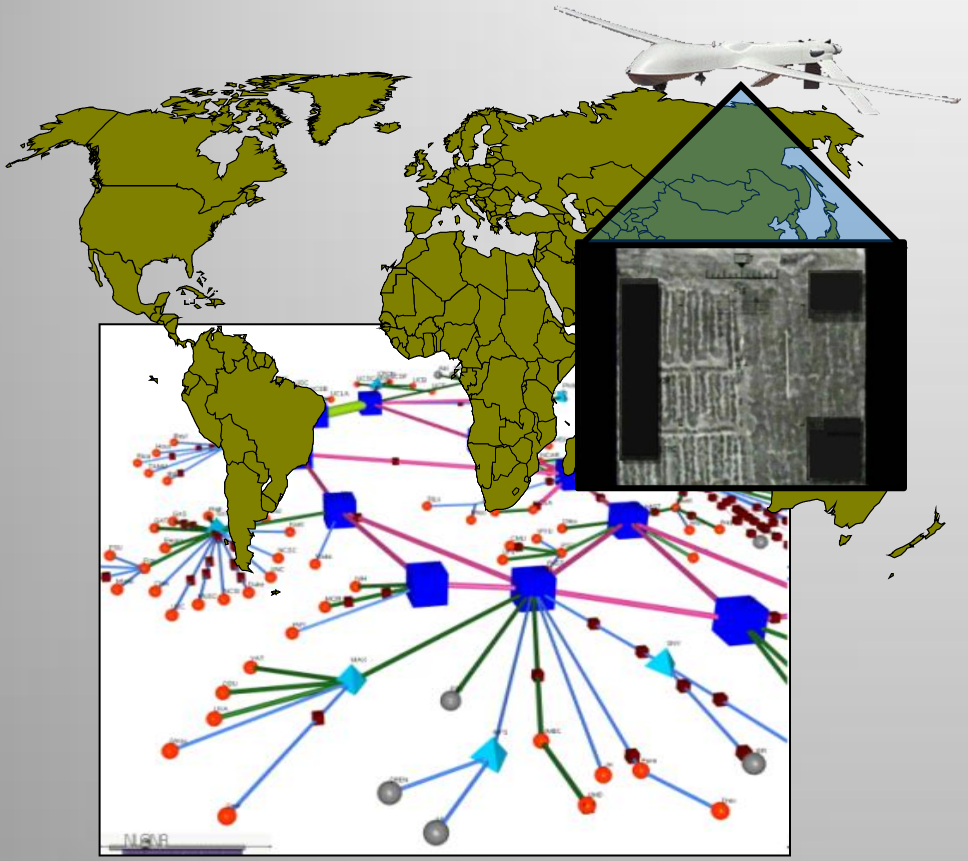
Nearer term: Assure missions in today's network (1-5 years)

- Situational awareness – models distributed over the full network
- Predictive simulation of network behaviors
- Adaptive defense to respond and recover in real-time (mission resilience)
- Human interfaces and elements – including both the adversary and the analyst in the model

Longer term: Enable deterrence and prevention (3-10 years)

- Attribution and deterrence – Focus on new identity technologies, policies, and international agreements. Use large scale simulation to design and evaluate.
- Supply chain assurance – Tools and methods for deep analysis of complex hardware, firmware, and software systems. Does the system do only what we expect?

Operations are informing the science – but the transition from science back to operations is critical



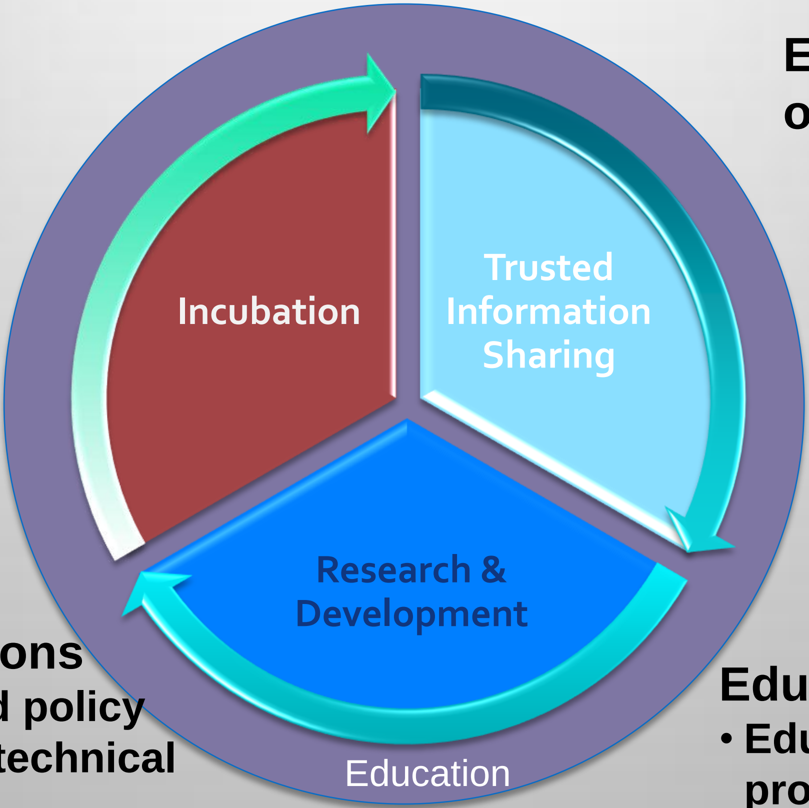
The DOE Labs are working together to develop government partnerships to transition R&D in

- **Network situational awareness**
  - Low-impact network mapping
  - Multisource network characterization
  - Real-time anomaly detection
- **Predictive network analysis**
  - Simulation for mission risk analysis
  - Rapid reverse engineering tools
  - Malware fingerprinting and attribution

The Network Security Innovation Center (NSIC) is a new industry and university focused partnership

Expanding the set of innovators

- Access to resources – computation, data, tools
- Enable broad participation in development
- Managed by UC Berkeley



Enabling secure operations

- Secure, authenticated threat information sharing
- Anchored by a trusted FFRDC
- Sharing product and best practices experience

Building R&D foundations

- Roadmaps for R&D and policy
- Workshops in focused technical areas
- Foundational R&D projects – technical refresh for the incubator

Education and outreach

- Education and outreach programs transition concepts into practice
- Workshops on technology-policy integration

Building and retaining workforce is one of our most critical issues

Issues …

- The US does not produce enough graduates in computer science and math
- In SF Bay Area we need a constant stream of recruiting
- Developing technical leadership in new areas

Programs

- CyberDefenders – joint summer student program with Sandia
- Visiting scientist and faculty program – build long-term university relationships
- Focused training programs