Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Modeling for Cyber Security and Cyber Resiliency

Nick Multari, PhD
Pacific Northwest National Laboratory
Richland, WA

Nick.multari@pnnl.gov

CNNMoney
A Service of CNN, Fortune & Money

FORTUNE | M

Home | Video | Business News | Markets | Investing | Economy | Tech

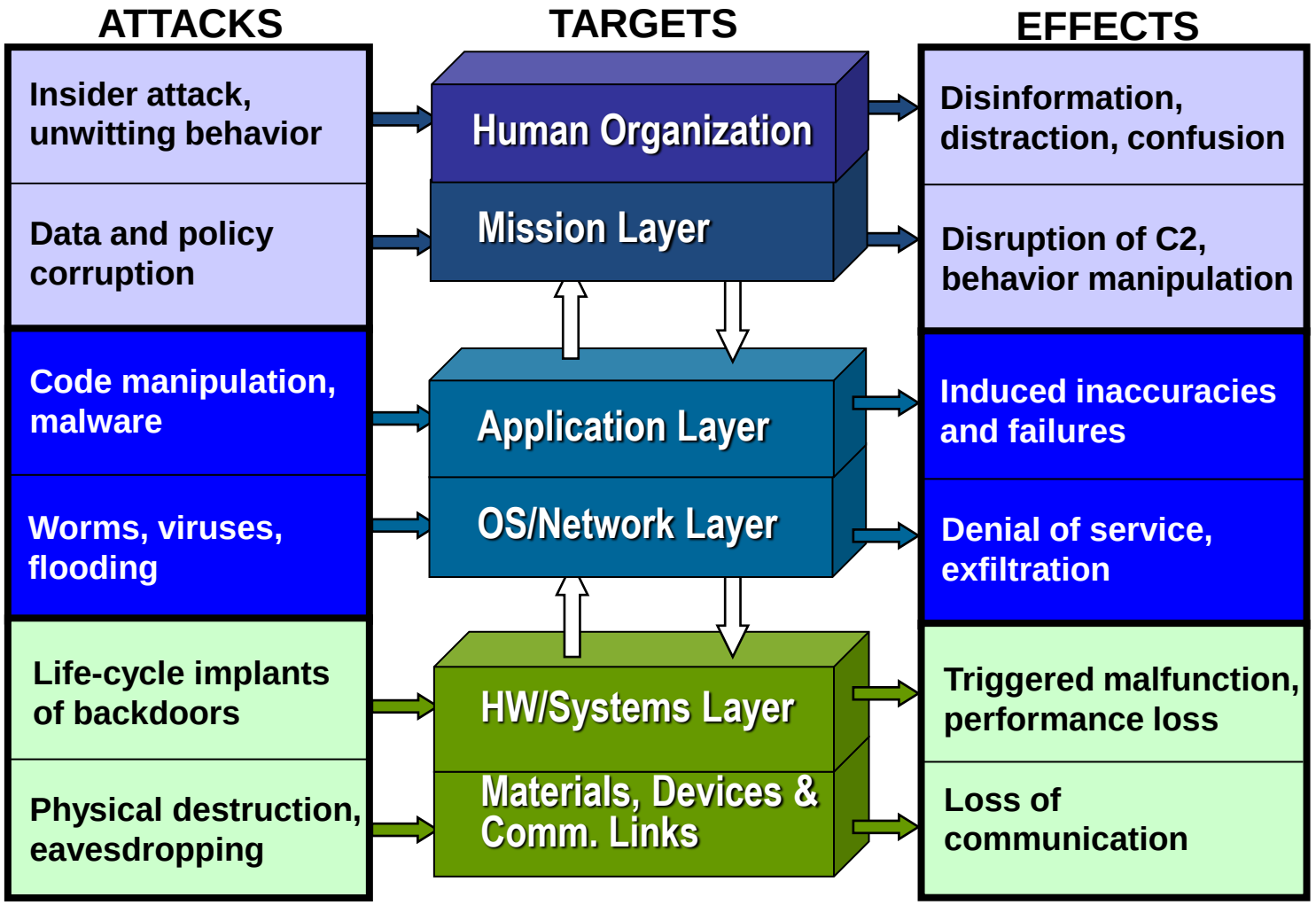
Mobile | Security | Social | Innovation | Enterprise | Apple 2.0 | Video

THE CYBERCRIME ECONOMY

Major banks hit with biggest cyberattacks in history

By David Goldman @CNNMoneyTech September 28, 2012: 9:27 AM ET

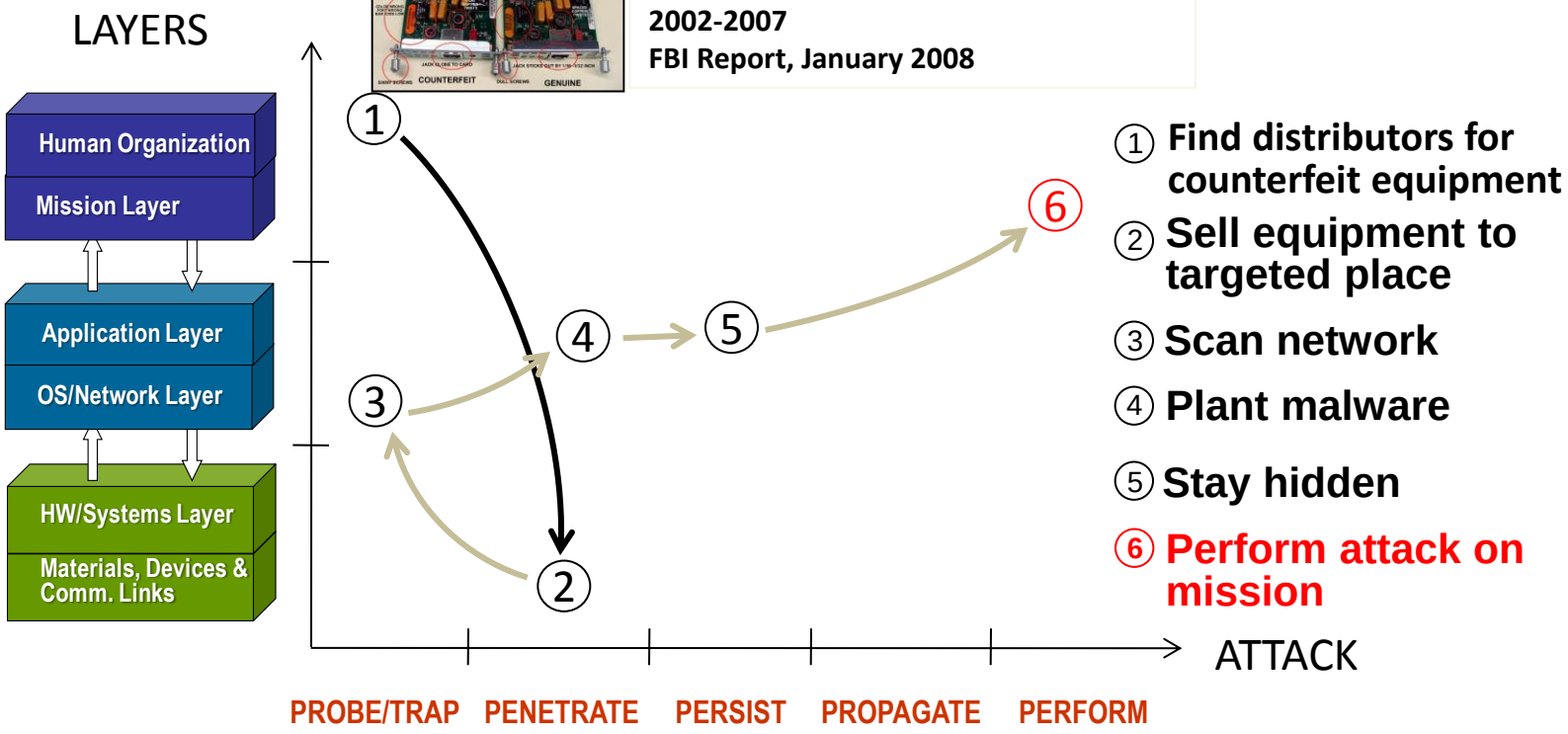
The Elements of a Contested Cyber Environment[1]



[1] 2008 AFSAB report "Defending and Operating in a Contested Cyber Domain"

Example for Attack Trajectories[2]

Counterfeit CISCO 1721 Router
1/5 of cost of original
2002-2007
FBI Report, January 2008



① **Find distributors for counterfeit equipment**
② **Sell equipment to targeted place**
③ **Scan network**
④ **Plant malware**
⑤ **Stay hidden**
⑥ **Perform attack on mission**

Attack trajectories are dynamic:
- **Depend on target and choose the least resistance**
- **May leave out layers (such as network layer)**
- **May change dynamically by reacting to defensive actions**

[2] 2008 AFSAB report "Defending and Operating in a Contested Cyber Domain"

Given sufficient time and resources, any perimeter and system can be breached

So, What's Needed?

- Need to know yourself
  - What is my mission?
  - What processes are critical to that mission?
  - What is the security posture of those processes?
  - How can I ensure those processes will continue operating even in face of a successful cyber attack?
- And, this information must be available in real-time

Security Modeling Using Large Scale Graphs

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Hypothesis

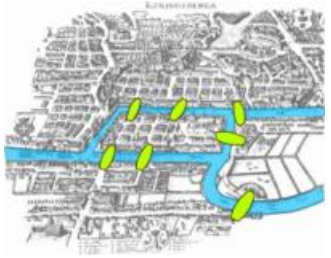
Large scale dynamic graphs capture the key processes in moving target defenses, while modeling these defenses for cyber enterprises

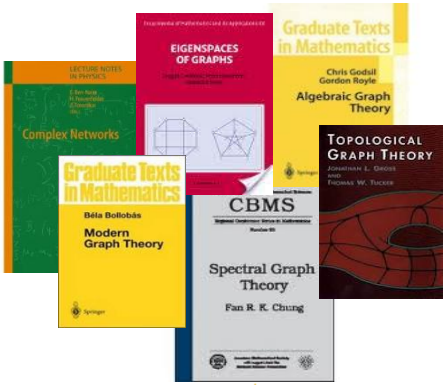
Challenge

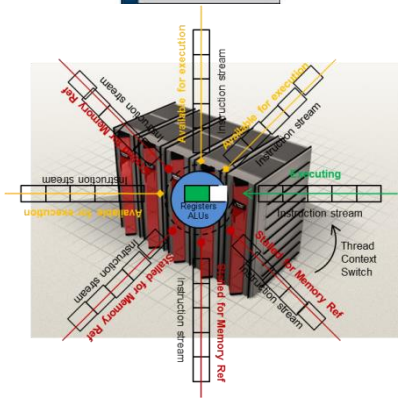
Creation of integrated graph/network model that can be updated at the velocity of the underlying network.

Advantage of Using Graph Representation

- A formal method and mathematical language to study cyber systems
  - Exploit graph theory, network theory, linear algebra and matrix theory
  - Formally discuss: *structure, mechanics, dynamics*
- Novelty and impact of approach
  - Dynamic graph as a model to perturb the system of study



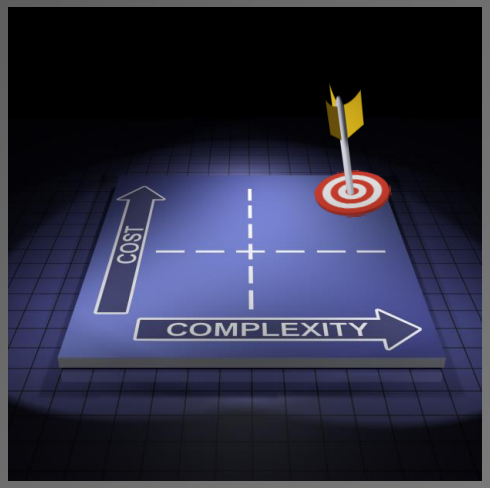




Multiscale Modeling is Needed

Hypothesis

Multi-scale modeling captures the essential features of graph models to enable the calculation of security posture and cost/benefit metrics

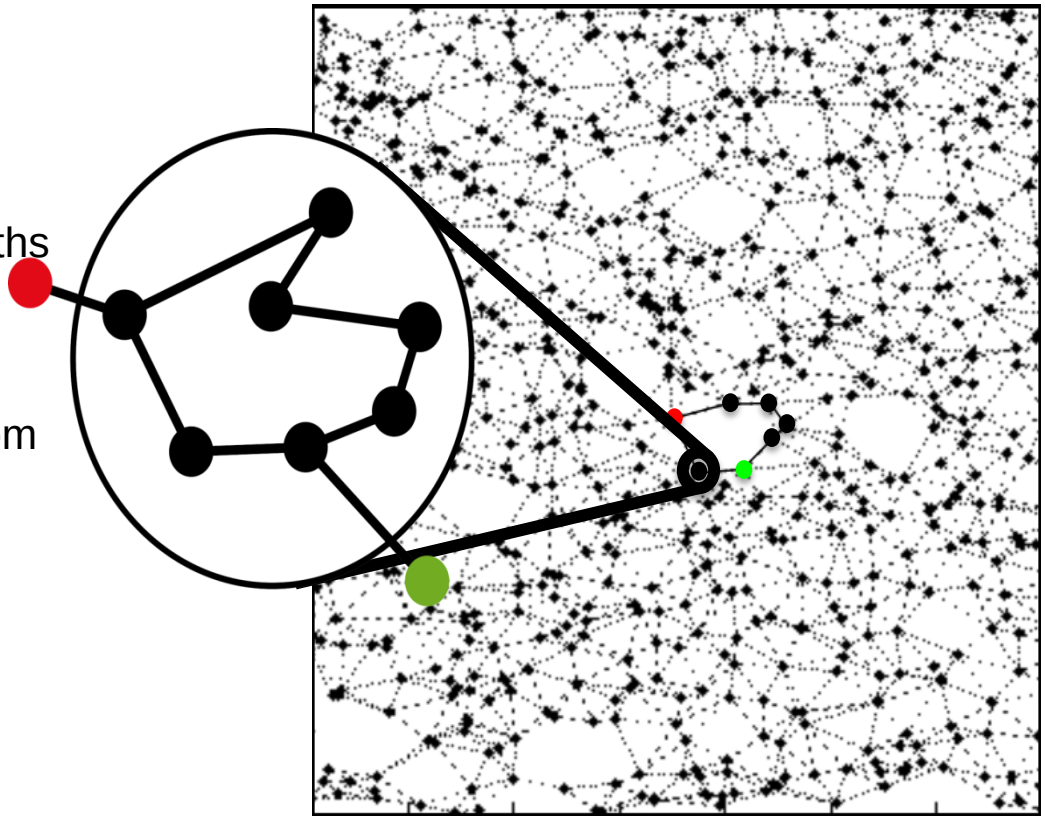


Challenge

Adaptation and creation of multiscale algorithms in the cyber environment to model the enterprise scale

New Techniques for Interacting with Multi-scale Graphs

- **Three dimensions**
  - Temporal
    - Events (e.g. attacks) cross timescales ranging from microseconds to months
  - Structural
    - Events (e.g. attacks) cross structural scales ranging from the entire network to processes on individual machines
  - Computational
    - Monte Carlo / Randomized Algorithms

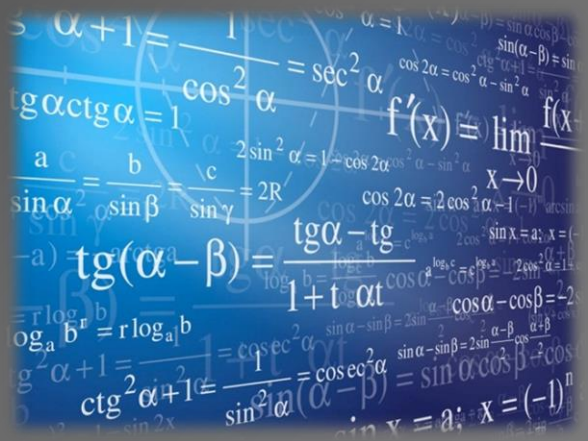


Metrics Complete the Picture

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Hypothesis

Graph and other measurable quantities can be used to capture the essential security posture and cost/benefit ratio in real time

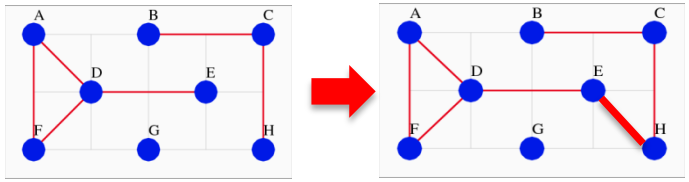


Challenge

- Large scale graphs are required
- Calculations must also keep up with velocity of moving target
- May need information not traditionally measured nor available

Deriving security metrics from a graph representation

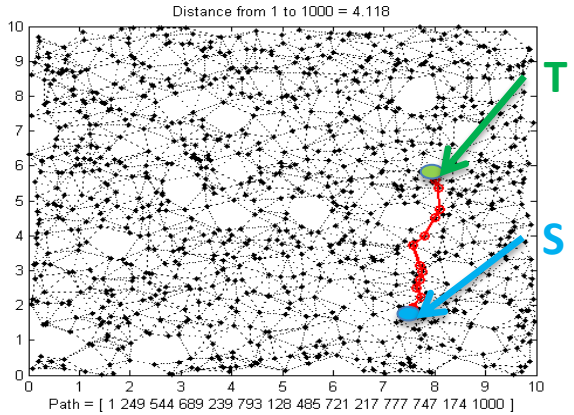
- **Elements of limited network-based understanding**
  - Structure
    - Physical structure provides limits
  - Mechanics
    - Physics of components, communication protocols
      and policies, both hardware and software, force distinct behaviors
  - Dynamics
    - Both structure and mechanics change over time



Structurally impossible to go from A to H

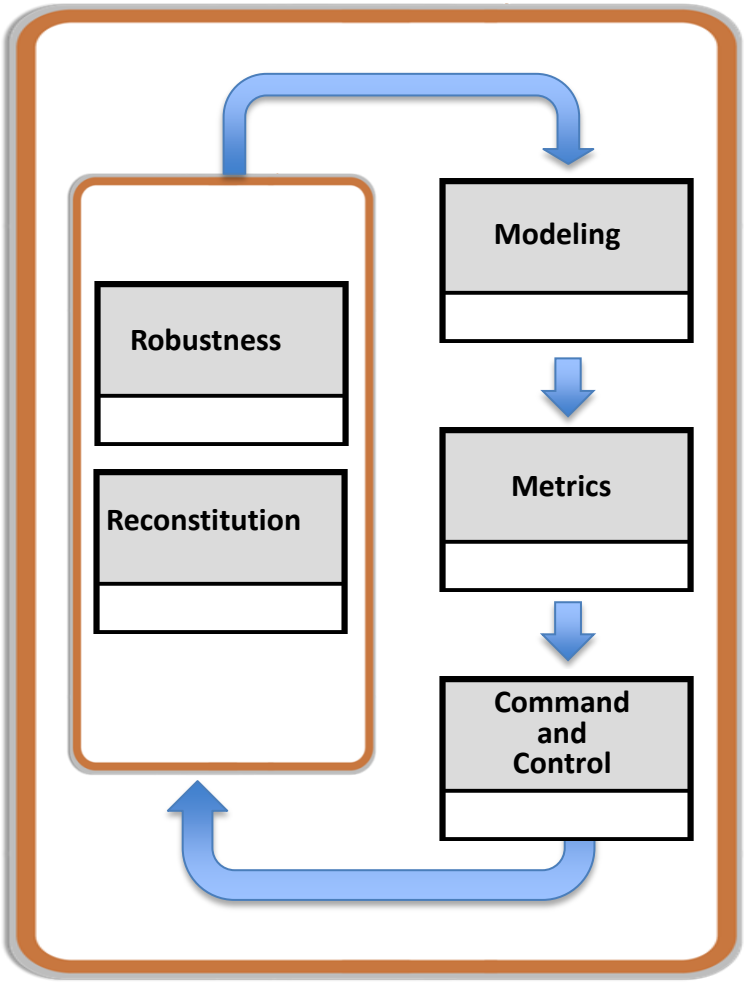
At time *t*, a new link is added between E and H

- **Models move this domain into quantitative and scientific space**
  - Cross section gives you a measure of risk – what is the likelihood of getting from S to T
  - Centrality informs path of motion – alter the probability of reaching T



Asymmetric Resilience

Asymmetric Resilience



In Short …

- Deterrence is key in reducing attempts but …
  Will never successfully defend against or stop all attacks
- Therefore, need to **know yourself** via …
  Models and Metrics
- To ensure critical functions **continue to operate** by …
  Designing theory-guided resilient systems
- All with the goal of …
  *Further improving deterrence by achieving an **asymmetric advantage** for the defender*