Transforming DOE Cyber Security

A Science-Based Approach

A report from the grass roots cyber security community

For the U.S. Department of Energy, Office of Science

Prepared by:

Deborah Frincke deborah.frincke@pnl.gov

Charlie Catlett catlett@anl.gov

Ed Talbot ebtalbo@sandia.gov

Brian Worley worley@ornl.gov

What others think . . .

The nation's critical infrastructure, such as the electric power grid, air traffic control system, financial system, and communication networks, depends extensively on information technology for its operation. Concerns about the vulnerability of this infrastructure have heightened in the security-conscious environment…
["Toward a Safer and More Secure Cyberspace," The National Academies]

… cheaper and easier to get hold of the tools needed to launch a cybercrime attack [RSA]

"Estonia was a wakeup call…We have to wake up our governments … If people do not understand the urgency now, they never will."
– Viviane Reding, EU Information Society commissioner

"We haven't implemented information security. We have been securing the perimeter, the moat and castle, but not the king, and information is the king. And like a king, information has a nasty habit of wanting to move around."
–Art Coviello, executive vice president, EMC and president, RSA

"Cyberspace is very important, very insecure and security problems are getting worse. For lots of reasons (economic, public safety, national security) it is very much in the broad public interest to make it safer and more secure." [National Academies]

3 Questions Launched the Community

1. What are the key priorities with regard to cyber security research and development over the next decade?

2. What would we recommend, in terms of a program, to address those priorities?

3. How would a DOE Office of Science program in this area complement other cyber security R&D initiatives such as NSF's or other agency programs?

First Community Workshop

February 11-13, 2008 at Argonne National Laboratory - 44 Participants

PNNL:
Frincke, Thompson

Ames:
Bode, Strasburg

UIUC:
Khurana

ANL:
Caltett, Swietlik, Engert, Rackow, Volmer, Kwiatkowski, Martin, North, Poetzel, Skwarek

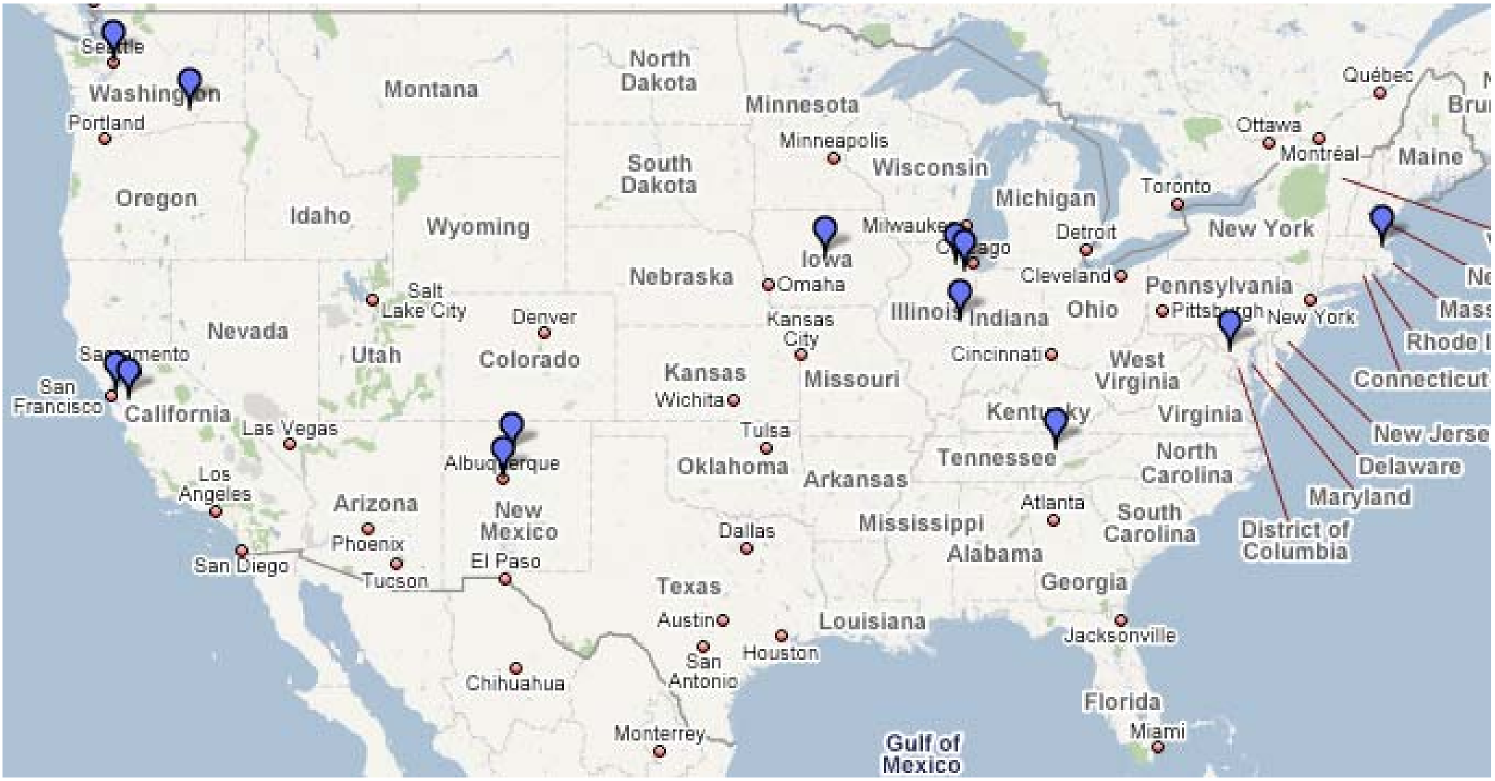
FNAL:
Altunay, Crawford, Cudzewicz, Gaines, Petravick

UW:
Endicott-Popovsky

LBL:
Agarwal, Draney, Stone, Lant

LLNL:
Quinlan, Sommer, White

SNL:
Talbot, Vanderveen



BBN:
Goldfarb

DOE:
Polansky

LANL:
VonderWiel, Wendelberger

SNL:
Armstrong, Berry, Minnich, Napolitano, Pundit

ORNL:
Griffin, Jiao, Wilder, Worley, Kemper

Office of Science
U.S. DEPARTMENT OF ENERGY

First Community Workshop

February 11-13, 2008 at Argonne National Laboratory - 44 Participants

PNNL:
Frincke, Thompson

Ames:
Bode, Strasburg

UIUC:
Khurana

ANL:
Caltett, Swietlik, Engert, Rackow, Volmer, Kwiatkowski, Martin, North, Poetzel, Skwarek

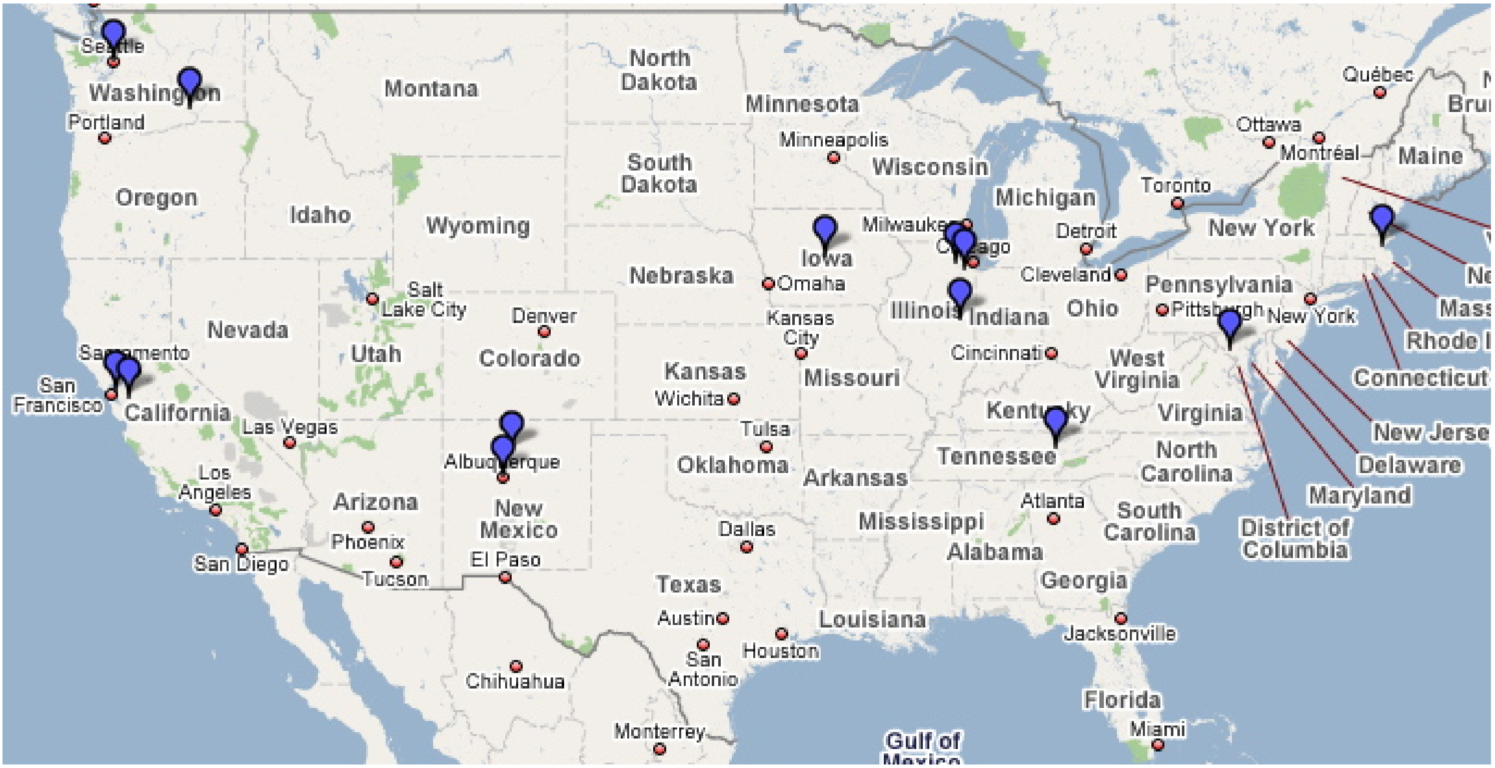
FNAL:
Altunay, Crawford, Cudzewicz, Gaines, Petravick

UW:
Endicott-Popovsky

LBL:
Agarwal, Draney, Stone, Lant

LLNL:
Quinlan, Sommer, White

SNL:
Talbot, Vanderveen



BBN:
Goldfarb

DOE:
Polansky

LANL:
VonderWiel, Wendelberger

SNL:
Armstrong, Berry, Minnich, Napolitano, Pundit

ORNL:
Griffin, Jiao, Wilder, Worley, Kemper

Office of Science
U.S. DEPARTMENT OF ENERGY

Findings[1]

- **Need** for investment in proactive long-term approach to Cyber Security.
- DOE has **a unique history** of taking on national priorities that involve long-term, sustained, focused research and development with clear mission-objectives.
- DOE's **science mission** supports operational laboratories, instruments, and other facilities.
- DOE can provide a broad-based **scientific approach** to cyber security through the national laboratory system.

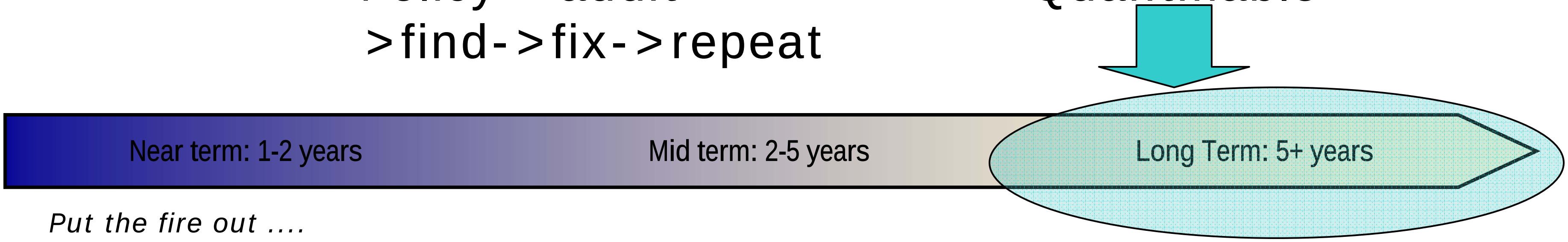
(1) D. Frincke, C. Catlett, F. Siebenlist, E. Talbot, R Strelitz, B. Worley*. Transforming CyberSecurity R&D within the DOE: Getting ahead of the threat,* Technical Report 0001 from the DOE cybersecurity grass roots community.

Office of Science
U.S. DEPARTMENT OF ENERGY

A Science-Based Approach:

- Move away from:
  - Largely reactive
  - Short term investments in engineered term solutions
  - Catch-n-patch
  - Policy->audit->find->fix->repeat

- Move towards:
  - Emphasize the proactive
  - Long term, visionary, transformational
  - Provable, testable
  - Quantifiable



Put the fire out ....

Install fire suppression sprinklers ...

Intrinsically fireproof buildings

Office of Science
U.S. DEPARTMENT OF ENERGY

Collaboration is KEY!

Our discussions, teleconferences, Town Hall meeting, and paper development are products of 40+ creative and dedicated individuals from:

- Ames Laboratory
- Argonne National Laboratory
- BBN Technologies
- U.S. Department of Energy
- National Energy Research Scientific Computing Center
- Sandia National Laboratories
- Pacific Northwest National Laboratory
- University of Washington
- Fermi National Accelerator Laboratory
- Invensys
- Lawrence Berkeley National Laboratory
- Lawrence Livermore National Laboratory
- Los Alamos National Laboratory
- University of Illinois at Champaign/Urbana
- Oak Ridge National Laboratory
- Colorado State University

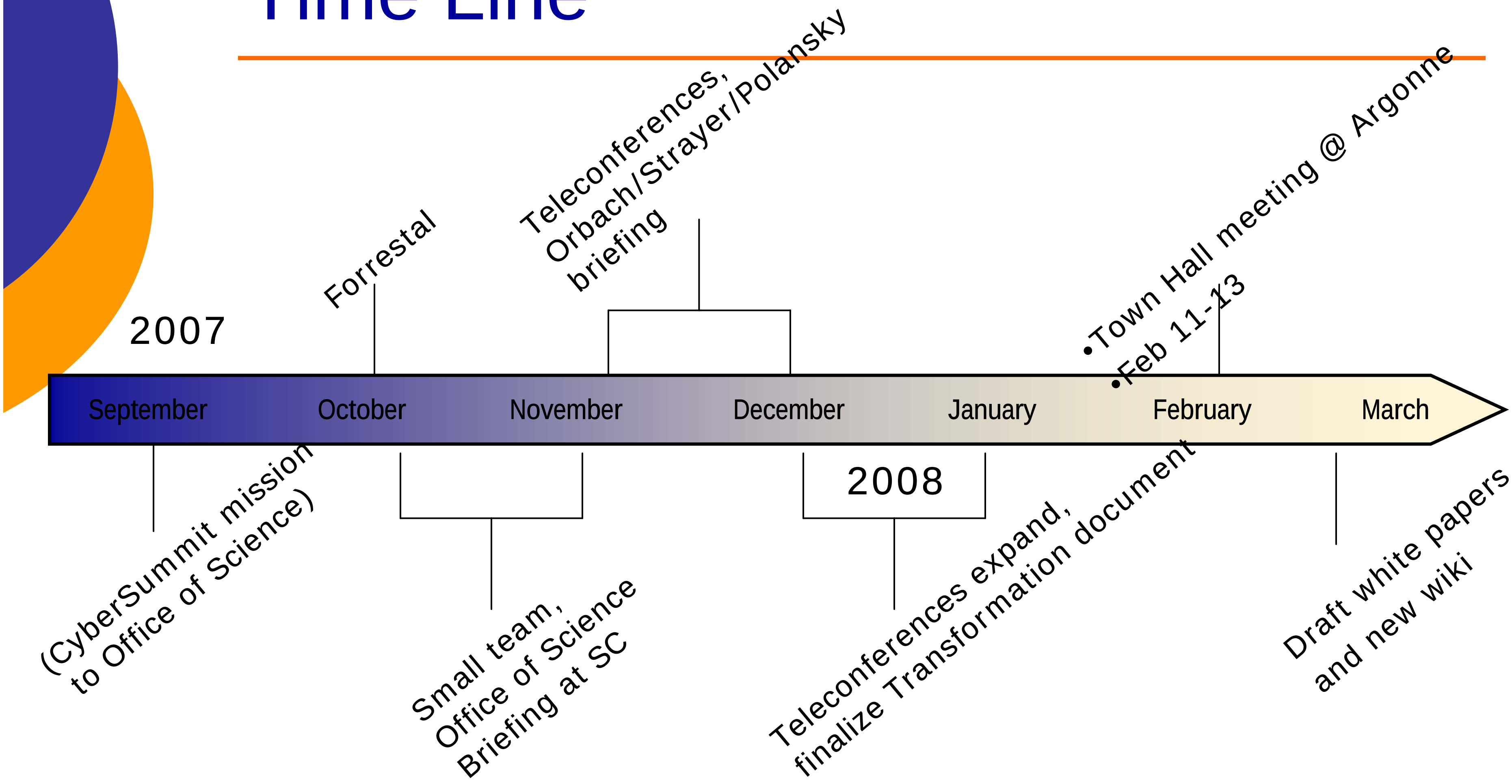
Office of Science
U.S. DEPARTMENT OF ENERGY

Goals and Objectives

"We will enable the DOE mission by transforming the ability of domain scientists to work safely, despite the need to operate within an insecure cyber-world."

- Advancing the state of the science
- Open Source and transparent
- Solicit high-level direction from the classified communities for their long term benefit.
- Strive for long-term and high-risk research directions
- Identify short-term payoffs
- Remain aware of and responsive to shifts in the industry and use of technology
- Be threat-agnostic
- Strive for benefits beyond the DOE missions
- Actively foster collaboration with commercial academia, and other government communities

Time Line



2007

September

October

November

December

January

February

March

2008

(CyberSummit mission to Office of Science)

Forrestal

Small team, Office of Science Briefing at SC

Teleconferences, Orbach/Strayer/Polansky briefing

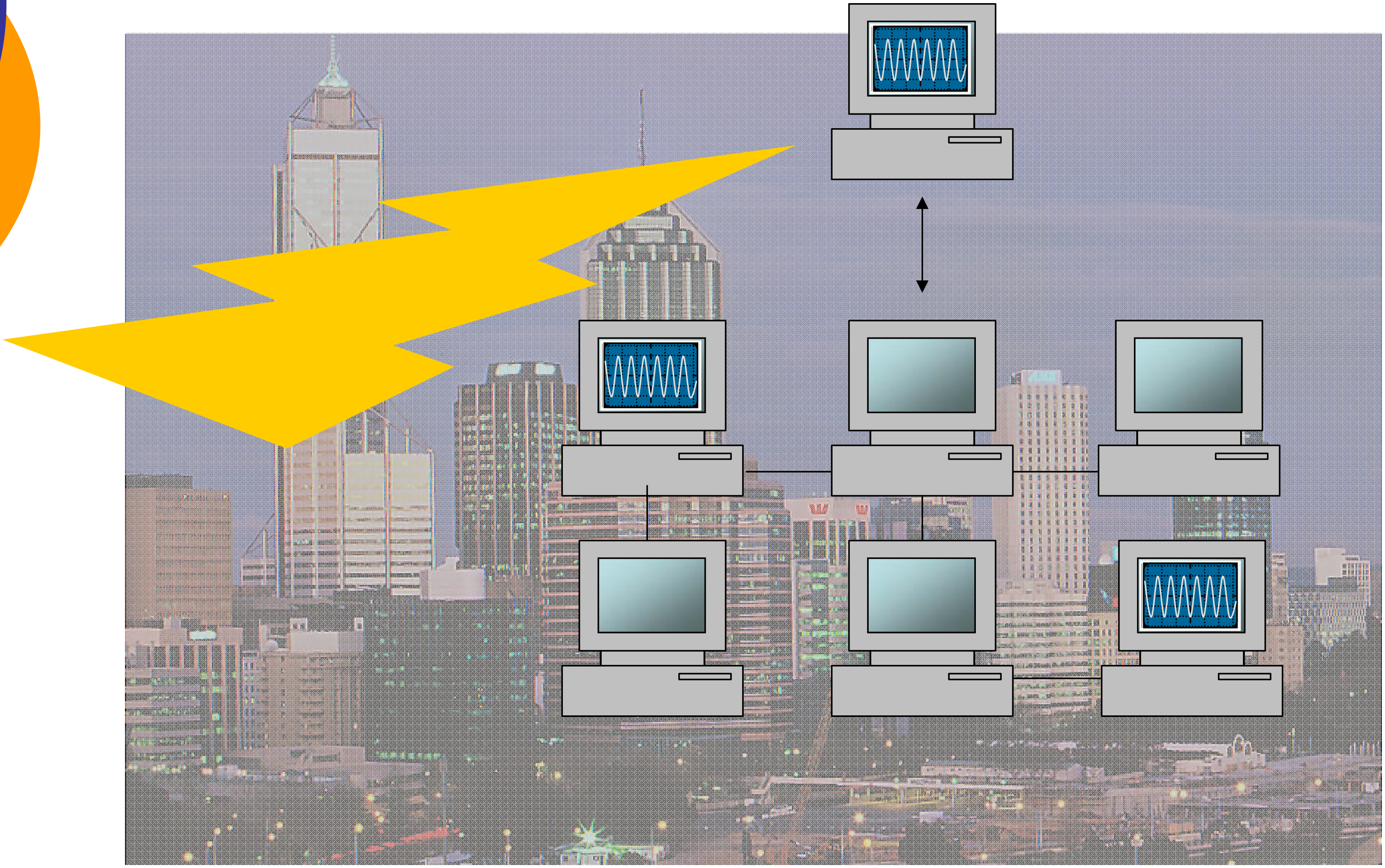
Teleconferences expand, finalize Transformation document

- Town Hall meeting @ Argonne
- Feb 11-13

Draft white papers and new wiki

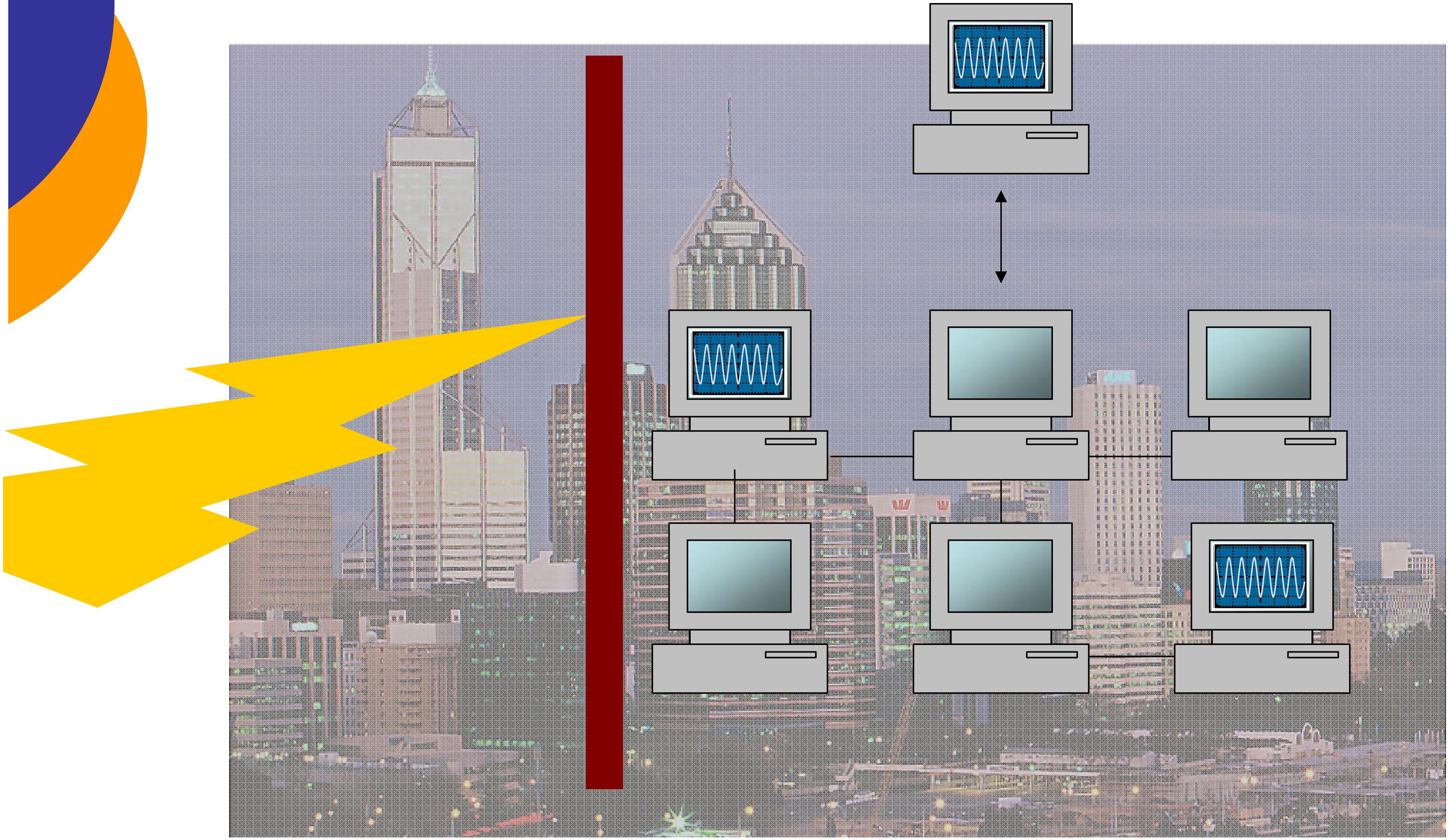
Currently planning "approximately April Town Hall Meeting

What if . . .



[redacted]

Changing the Game



Ahead of the Threat

Predicting the actions of an adversary

Computer Science	Rapid integration and parsing of heterogeneous, very large scale data sets	Simulation/ modeling (consequences)	Collaborative situational awareness	Data pedigree	Pairwise gene similarity computation
Mathematics	Network tomography; Very large graphs; scale free networks	Matrix/tensor methods for criticality	Byzantine agreement	Game theory	Risk analysis and reliability theory Dempster-Schaefer evidence equations
Computer Hardware	Verifiably correct/secure hardware components	Policy/privacy aware sensors for hostile environments	Secure and performance-sensitive command/control systems	Secure multicore systems	Integrity for very large scale file systems

Office of Science
U.S. DEPARTMENT OF ENERGY

Ahead of the Threat

Self Healing and Resilient Systems

Computer Science	Rapid integration and parsing of heterogeneous, very large scale data sets	Simulation/ modeling (consequences)	Collaborative situational awareness	Data pedigree	Pairwise gene similarity computation

Mathematics	Network tomography;
	Very large graphs;
	scale free networks
		Matrix/tensor methods for criticality	Byzantine agreement	Game theory	Risk analysis and reliability theory Dempster-Schaefer evidence equations

Computer Hardware	Verifiably correct/secure hardware components	Policy/privacy aware sensors for hostile environments	Secure and performance-sensitive command/control systems	Secure multicore systems	Integrity for very large scale file systems

Documents and Writings

- Document: Transforming Cyber Security
  - What are the key priorities with regard to cyber security research and development over the next decade?
  - What would we recommend, in terms of a program, to address those priorities?
  - How would a DOE Office of Science program in this area complement other cyber security R&D initiatives such as NSF's or other agency programs?
- White papers and demonstrations: in progress
- Call coming “soon”: Special Edition Journal
- Wiki: in use by the community

Numerous participants helped write *Transforming CyberSecurity*!

- Section 1: *Science-based Cyber Security Research Priorities for the Next Decade*
  - F. Siebenlist (ANL), C. Catlett (ANL), D. Frincke (PNNL), E. Talbot (SNL), D. Petravik (FNL), T. Bartoletti (LLNL)

- Section 2: *Structure and Components*
  - *R. Strelitz (LANL), E. Talbot (SNL), D. Frincke (PNL), C. Catlett (ANL), M. McQueen (INL)*

- *Section 3: Overview of Synergistic Programs and Research Directions for the Department of Energy*
  - *B. Worley (ORNL), C. Matarazzo (LLNL), Frincke (PNNL), T. Thompson (PNNL)*

- Deb Agarwal, Lawrence Berkeley National Laboratory
- Mine Altunay, Fermi National Accelerator Laboratory
- Robert Armstrong, Sandia National Laboratories (CA)
- Tony Bartoletti, Lawrence Livermore National Laboratory
- Patrick Burns, Colorado State University
- Charlie Catlett, Argonne National Laboratory
- Matt Crawford, Fermi National Accelerator Laboratory
- Susan Estrada, Aldea
- Ian Foster, Argonne National Laboratory
- Deborah Frincke, Pacific Northwest National Laboratory
- Mark Kaletka, Fermi National Accelerator Laboratory
- Celeste Matarazzo, Lawrence Livermore National Laboratory
- Miles McQueen, Idaho National Laboratory
- Leonard Napolitano, Sandia National Laboratories (CA)
- Don Petravick, Fermi National Accelerator Laboratory
- Anne Schur, Pacific Northwest National Laboratory
- Frank Siebenlist, Argonne National Laboratory
- Mike Skwerak, Argonne National Laboratory
- Joe St Sauver, University of Oregon
- Richard Strelitz, Los Alamos National Laboratory
- Craig Swietlik, Argonne National Laboratory
- Edward Talbot, Sandia National Laboratories (CA)
- Troy Thompson, Pacific Northwest National Laboratory
- Keith Vanderveen, Sandia National Laboratories (CA)
- Brian Worley, Oak Ridge National Laboratory

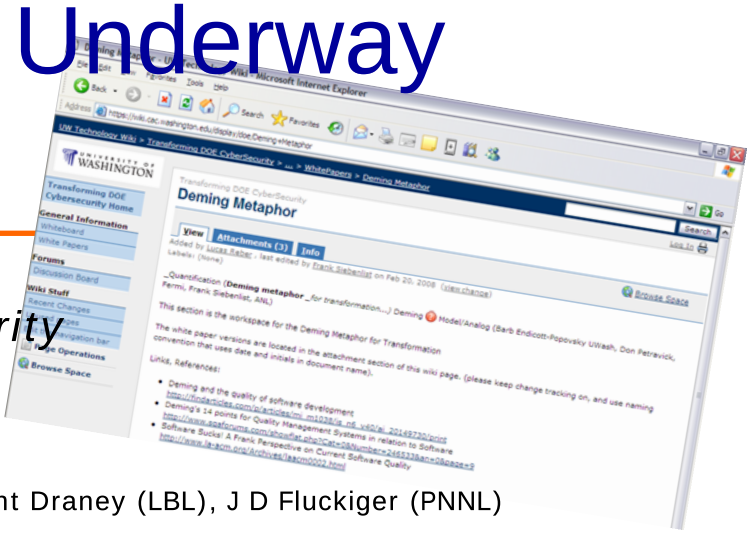
Recommendations from *Transforming CyberSecurity:*

- Section 1: *Science-based Cyber Security Research Priorities for the Next Decade*
  - F. Siebenlist (ANL), C. Catlett (ANL), D. Frincke (PNNL), E. Talbot (SNL), D. Petravik (FNL), T. Bartoletti (LLNL)
- Section 2: *Structure and Components*
  - *R. Strelitz (LANL), E. Talbot (SNL), D. Frincke (PNL), C. Catlett (ANL), M. McQueen (INL)*
- *Section 3: Overview of Synergistic Programs and Research Directions for the Department of Energy*
  - *B. Worley (ORNL), C. Matarazzo (LLNL), Frincke (PNNL), T. Thompson (PNNL)*

- R&D:
  - Open science security architecture for an exascale future
  - Multi-layer security understanding, awareness and response
  - Human aspects/factors & federated trust
  - Intrinsically secure control of critical systems
- Structure and components
  - Matrix not pipeline
  - Broad science base
  - Balance needs of open science with secrecy

Nine White Papers Underway

(authors & discussion participants)



https://wiki.cac.washington.edu/display/doe/Deming+Metaphor

Transforming DOE CyberSecurity

Deming Metaphor

Added by Lucas Reber , last edited by Frank Siebenlist on Feb 20, 2008 (view change)
Labels: (None)

_Quantification (**Deming metaphor** _for transformation...) Deming Model/Analog (Barb Endicott-Popovsky UWash, Don Petravick, Fermi, Frank Siebenlist, ANL)

This section is the workspace for the Deming Metaphor for Transformation

The white paper versions are located in the attachment section of this wiki page. (please keep change tracking on, and use naming convention that uses date and initials in document name).

Links, References:

- Deming and the quality of software development http://findarticles.com/p/articles/mi_m1038/is_n6_v40/ai_20149730/print
- Deming's 14 points for Quality Management Systems in relation to Software http://www.sqaforums.com/showflat.php?Cat=0&Number=246533&an=0&page=9
- Software Sucks! A Frank Perspective on Current Software Quality http://www.la-acm.org/Archives/laacm0002.html

- Complete *Transforming CyberSecurity*
- A Compelling Demo: Bios
  - Ron Minnich (SNL)
- Chronology
  - Chris Strasburg (Ames), Craig Lant (NERSC), Brent Draney (LBL), J D Fluckiger (PNNL)
- Classified Community
  - Brian Worley (ORNL), Chris Griffin (ORNL), Irwin Gaines (Fermi)
- Computer Science Challenges
  - Rob Armstrong (SNL) ; Chris Griffin (ORNL), Ron Minnich (SNL), Mine Altunay (Fermi)
  - Dan Chavarria (PNNL)
- Deming Metaphor
  - Barbara Endicott-Popovsky (U Wash); Don Petravick (Fermi); Frank Siebenlist (ANL)
- Mathematical Underpinnings
  - Joanne Wendelberger (LANL), Ed Talbot (Sandia), Louis Wilder (Oak Ridge), Yu Jiao Tamara (Oak Ridge), Kolda (Sandia)
  - Juan Meza (LBL), Deb Agarwal (LBL),Chad Scherrer (PNNL)
- Practical Answers
  - Matt Crawford (Fermi), Mine Altunay(Fermi), Barb Endicott-Popovsky (U Wash), Anne Schur (PNNL) ; Kirk Bailey (U Wash)
- Socratic and Thematic Approaches
  - Ed Talbot (SNL), Irwin Gaines (Fermi), Richard Strelitz (LANL), Troy Thompson (PNNL)

https://wiki.cac.washington.edu/display/doe/WhitePapers

DOE Cyber Security R&D

Grand Challenges | Discovery Research | Use-Inspired Basic Research | Applied Research | Technology Development & Deployment

Grand Challenges

- Provide continuing streams of new knowledge, advances, tools, technologies and protocols needed to protect the Department's assets from cyber attack through 2025.
- Mathematical Underpinnings
- Vet with stakeholders in other agencies, academia, and the "classified community"

Discovery Research

- Basic research to revolutionize approaches to cyber security.
- Research to develop innovative tools, strategies, technologies or techniques for cyber security.

Use-Inspired Basic Research

- Basic research to strengthen the DOE's current cyber architecture, usually in recognition of addressing potential showstoppers associated with legacy systems.

Applied Research

- Research with the goal of meeting *technical milestones*, with emphasis on the development, performance, life cycle cost, reliability and maintainability
- Proof of technology concepts

Technology Development & Deployment

- Scale-up research
- At-scale demonstration
- Cost reduction
- Prototyping
- Validation and verification
- Deployment
- Operations

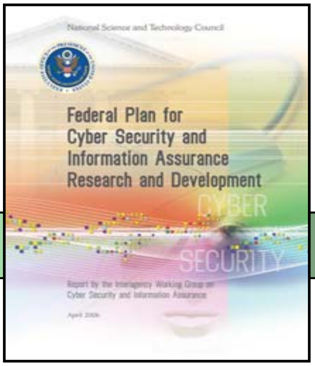
DOE Mission Contributions

Science R&D Defense Business Systems

Report of the Cyber Security Research Needs for Open Science Workshop
July 23-24, 2007
Energy Reliability

Basic Research Needs Workshops

Town Hall Meetings


National Science and Technology Council
Federal Plan for Cyber Security and Information Assurance Research and Development
CYBER
SECURITY
Report by the Interagency Working Group on Cyber Security and Information Assurance
April 2006

American Competitiveness Initiative
Leading the World in Innovation
Domestic Policy Council
Office of Science and Technology Policy
February 2006

National Priorities

Findings from *Transforming CyberSecurity*

- **Need** for investment in proactive long-term approach to cyber security

- DOE has a unique history of taking on national priorities that involve long-term, sustained, focused research and development with **clear mission-objectives**

- DOE's **science mission** is unique in that it directly supports operational laboratories, instruments, and other facilities.

- ***DOE can provide a broad based scientific approach*** to cyber security through the national laboratory system.

Office of Science
U.S. DEPARTMENT OF ENERGY

On the Horizon for the community

- Planning an open science program with broadly vetted science underpinnings to provide a strong foundation upon which to build operational cyber security policies and capabilities.

- Continuing to incorporate considerations for both the open science initiative, power grid and control systems, and the classified needs of the DOE.

- Workshops over the next several months continue to identify R&D priorities in terms of near- and long-term timeframes, resulting in a 10+ year roadmap.

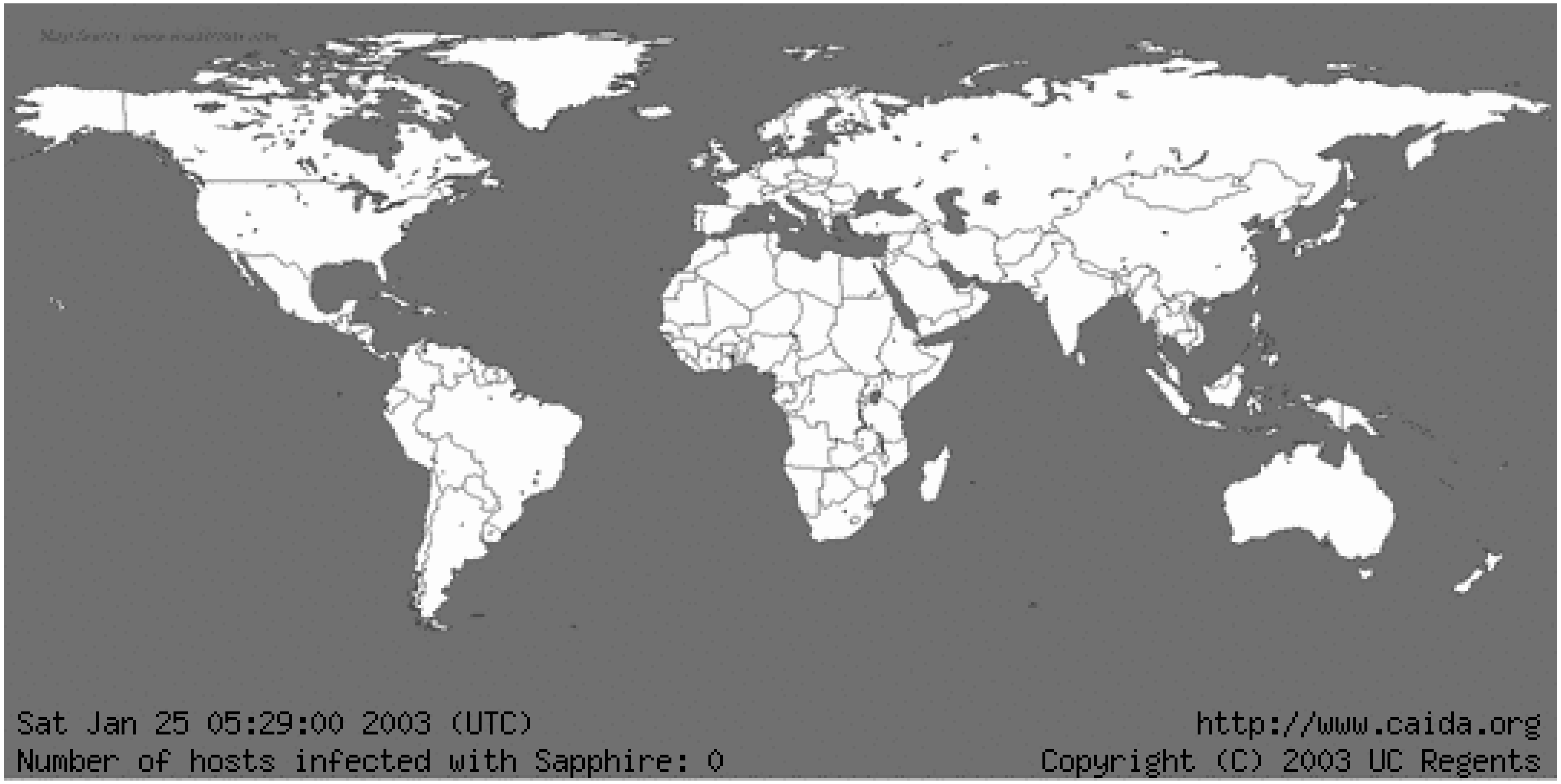
  Interactions among open, classified, power grid etc communities

  R&D uniqueness and integration with OGAs, academia, industry

  What might a funded program look like?

Office of Science
U.S. DEPARTMENT OF ENERGY

In Less Time Than We Have Spent Today


Sat Jan 25 05:29:00 2003 (UTC)
Number of hosts infected with Sapphire: 0
http://www.caida.org
Copyright (C) 2003 UC Regents

Source: http://www.caida.org/research/security/sapphire/

Office of Science
U.S. DEPARTMENT OF ENERGY

Questions?

Deborah A. Frincke
Deborah.frincke@pnl.gov

Charlie Catlett
Catlett@anl.gov

Ed Talbot
Ebtalbo@sandia.gov

Brian Worley
Worley@ornl.gov

Supplementary Slides

Additional detail available upon request.

Town Hall Meeting: More Details on R&D Areas (not in priority order)

Data Integrity, Availability, & Provenance

- -bit error rate as measure?
- -pedigree (who & how)
- -multiple administrative domains

Automated Screening of Software

- -dynamic & static analysis
- -computational & brute force
- -binary, source, runtime

Defendable networks

- -Forensically-ready networks
- -anomaly/intrusion detection
  - -active response, incident data sharing
- -policy-based monitoring
- -Cooperative detection/mitigation, automation

Secure Open Platform

- -chipset, bios, OS, architecture
- -Collaboration w/ COTS vendors

Measuring Security

- -Collaboration w/ OGAs
- -future operational context
- -units
- -dimensionality (confidentiality, availability, integrity…)
- -data mining
- -risk (QMU)
- -Deming QA

System Securability

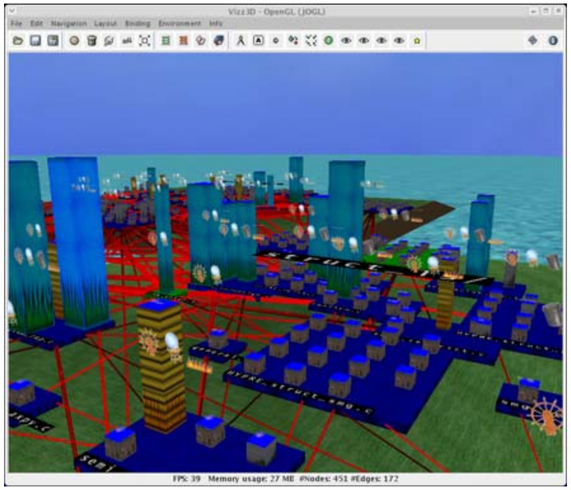
- -Definitions/Taxonomy
- -Trusted system out of untrusted components
- -Trust & Trust Management
- -Human Factors

Security Containers

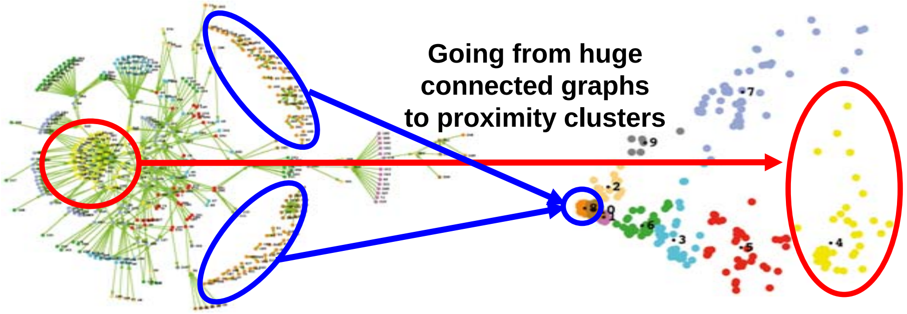
- -Virtualization
- -Controlling Complexity

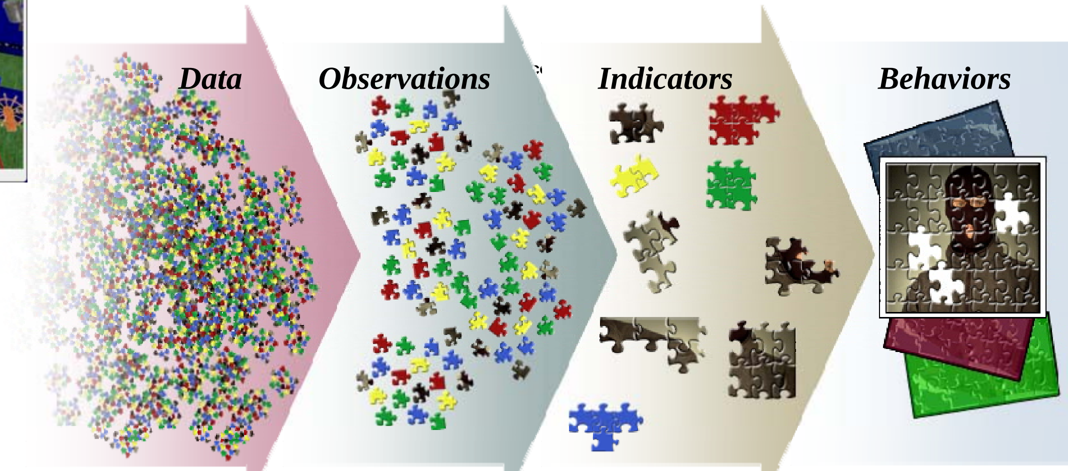
Office of Science
U.S. DEPARTMENT OF ENERGY

Mathematical Approaches



FPS: 39 Memory usage: 27 MB #Nodes: 451 #Edges: 172


Going from huge connected graphs to proximity clusters

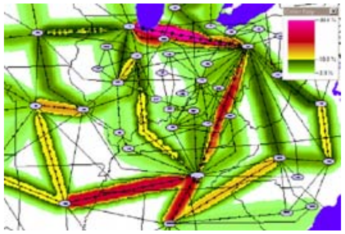


Incoming data processed to infer observations

Observations processed to infer indicators

Indicators assessed to gauge threat

Discover and associate actions that fit a malicious exploit profile

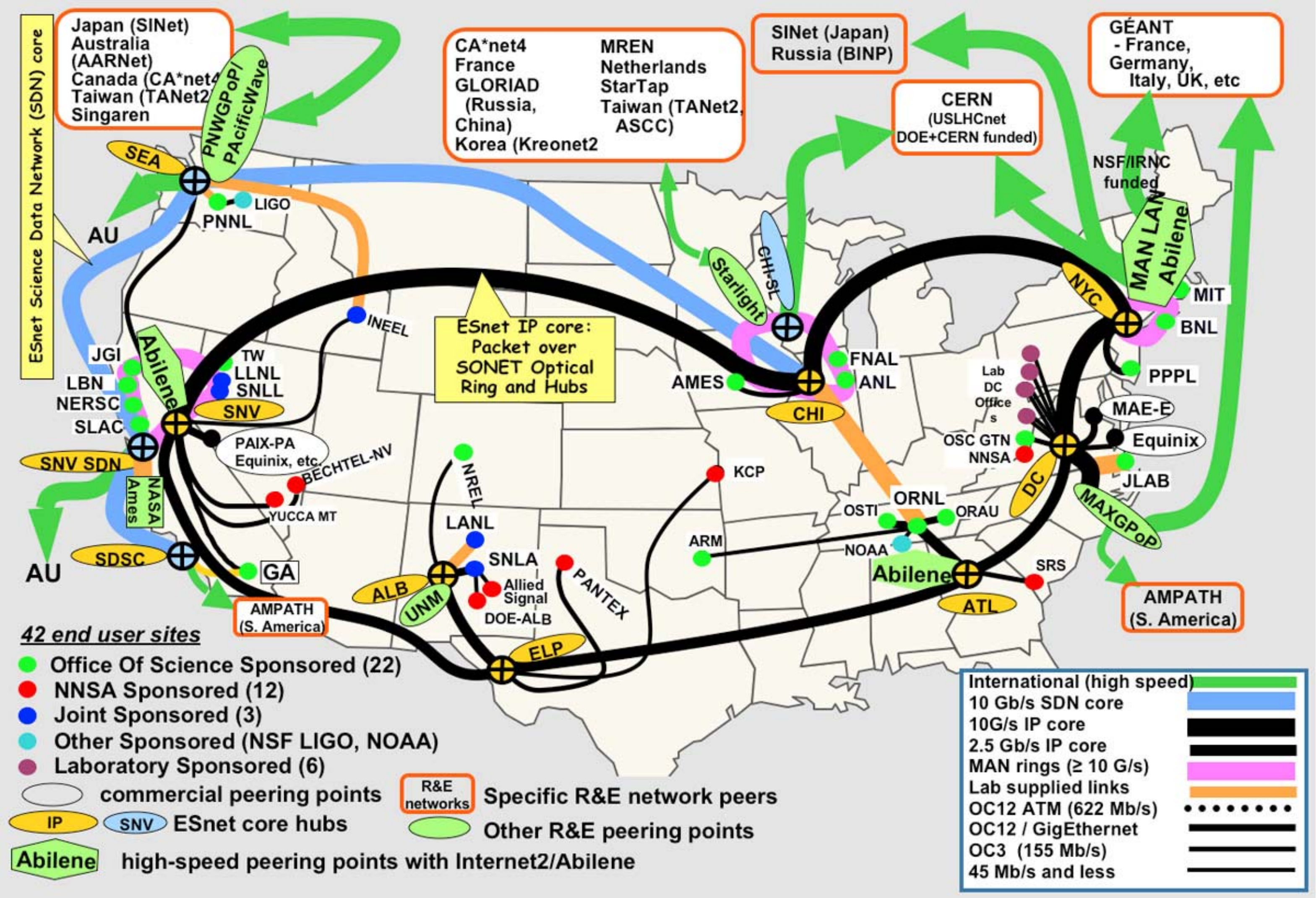


Visualizing a collection of transmission system lines

Office of Science
U.S. DEPARTMENT OF ENERGY

Complicated Security Requirements!

ESNET *(Fall, 2006)*



42 end user sites

- ● Office Of Science Sponsored (22)
- ● NNSA Sponsored (12)
- ● Joint Sponsored (3)
- ● Other Sponsored (NSF LIGO, NOAA)
- ● Laboratory Sponsored (6)
- ○ commercial peering points
- IP SNV ESnet core hubs
- Abilene high-speed peering points with Internet2/Abilene
- R&E networks Specific R&E network peers
- Other R&E peering points

International (high speed)	🟩
10 Gb/s SDN core	🟦
10G/s IP core	▬
2.5 Gb/s IP core	▬
MAN rings (≥ 10 G/s)	🟪
Lab supplied links	🟧
OC12 ATM (622 Mb/s)	•••••••
OC12 / GigEthernet	―
OC3 (155 Mb/s)	―
45 Mb/s and less	―