Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Experiment, Test, and Assessment Platform

DAVID MANZ

Asymmetric Resilient Cybersecurity Initiative Roadshow

May 12, 2017

Science of Cyber Security

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- **Need**
  - Confidence in measurements, mechanics, and prediction in cyberspace
- **Problem**
  - Treating as applied science without fundamental science foundation

Science of Cyber Security

- **Approach**
  - Methods for performing rigorous scientific research
  - Theories for the field to begin building a body of knowledge
  - Review field for successful research

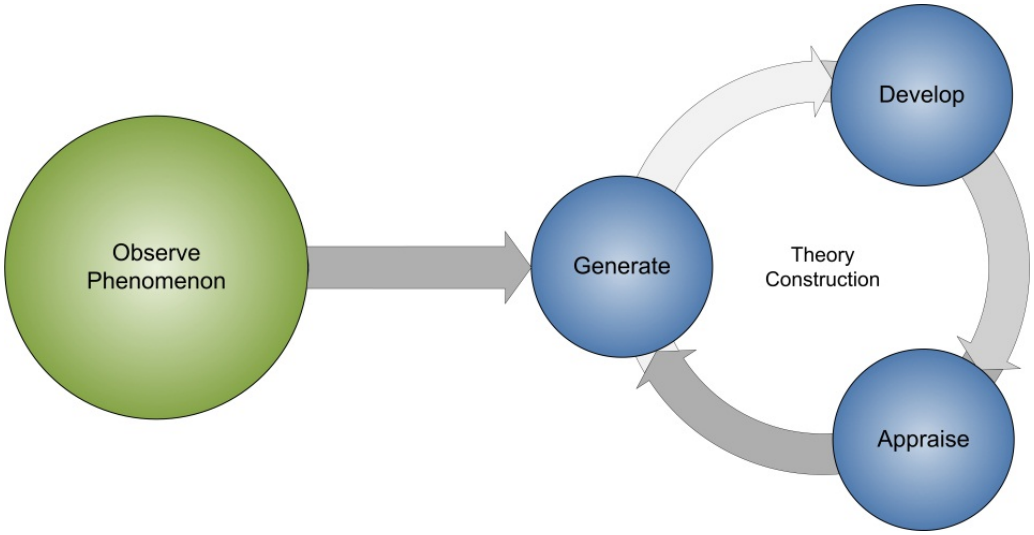
Science of Cyber Security

- **Benefit**
  - Move toward symmetry for defender
  - Enable metrics – ability to meaningfully measure
  - Support decision making
  - Grand challenge: Prediction

Cyber Security Scientific Methods

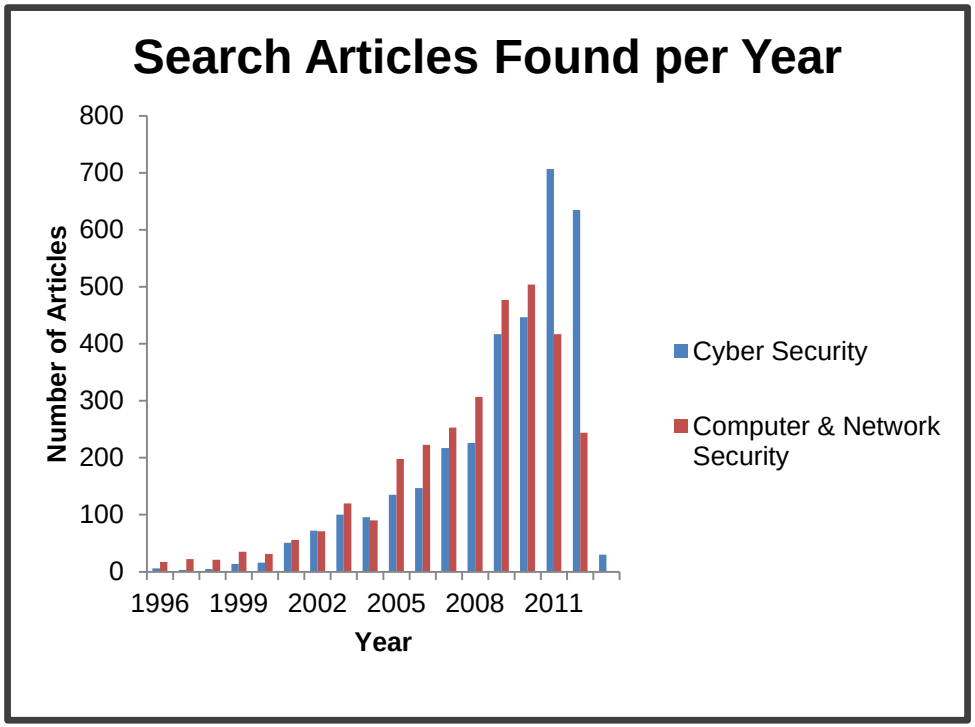
- Survey of other scientific fields
  - Medicine, physical sciences, social sciences, etc.

- Theory created from generation process
  - Inductive (generate ideas for theories from community datasets)
  - Abductive (reduce set of theories to most likely with additional datasets)
  - Hypothetico-deductive (design and execute experiment to test theory)



Progress to Date

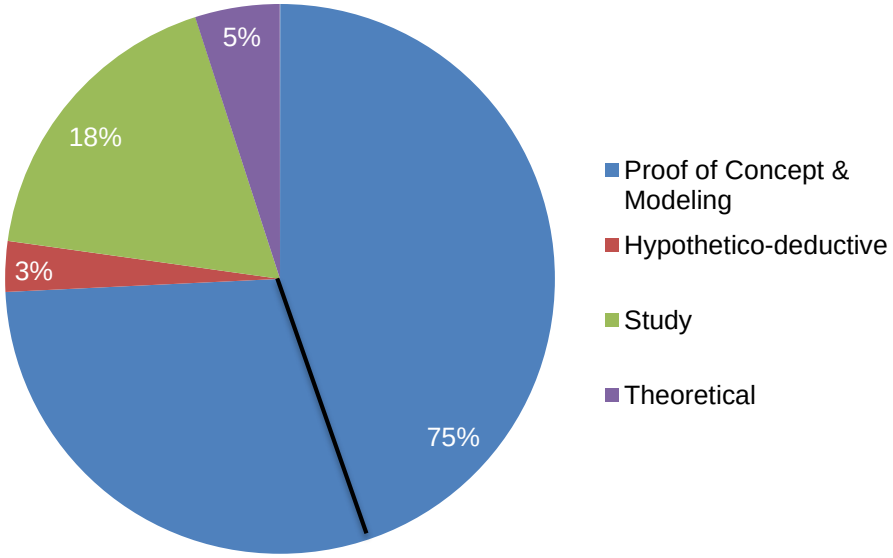
- Following method outlined by Tichy et al[1] and Wainer et al[2]
- Sources: ACM, IEEE, etc.
- Search terms (15 years)
  - Cyber security or cybersecurity
  - Network security
  - Computer security
- 5645 documents collected



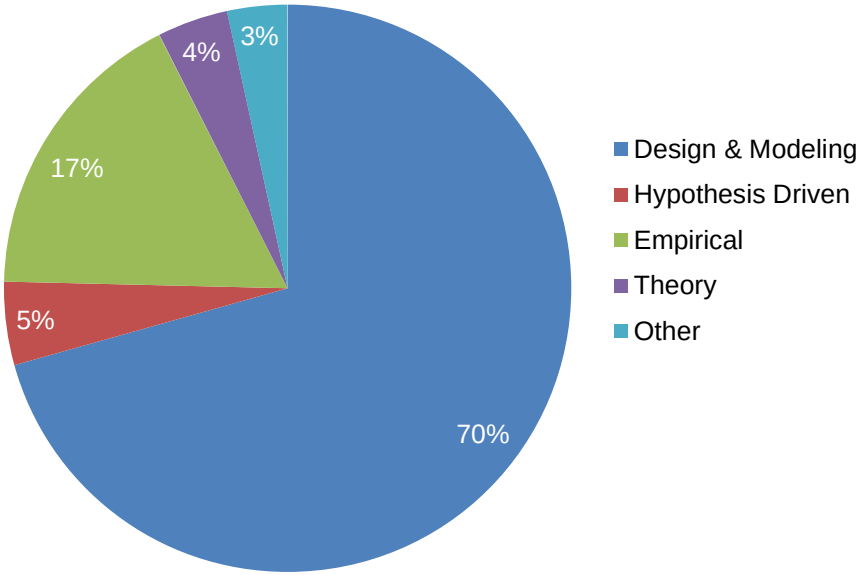
Preliminary Results Continued

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

PNNL Preliminary Results Merged



2009 Computer Science Study



Need for Experimental Testbeds

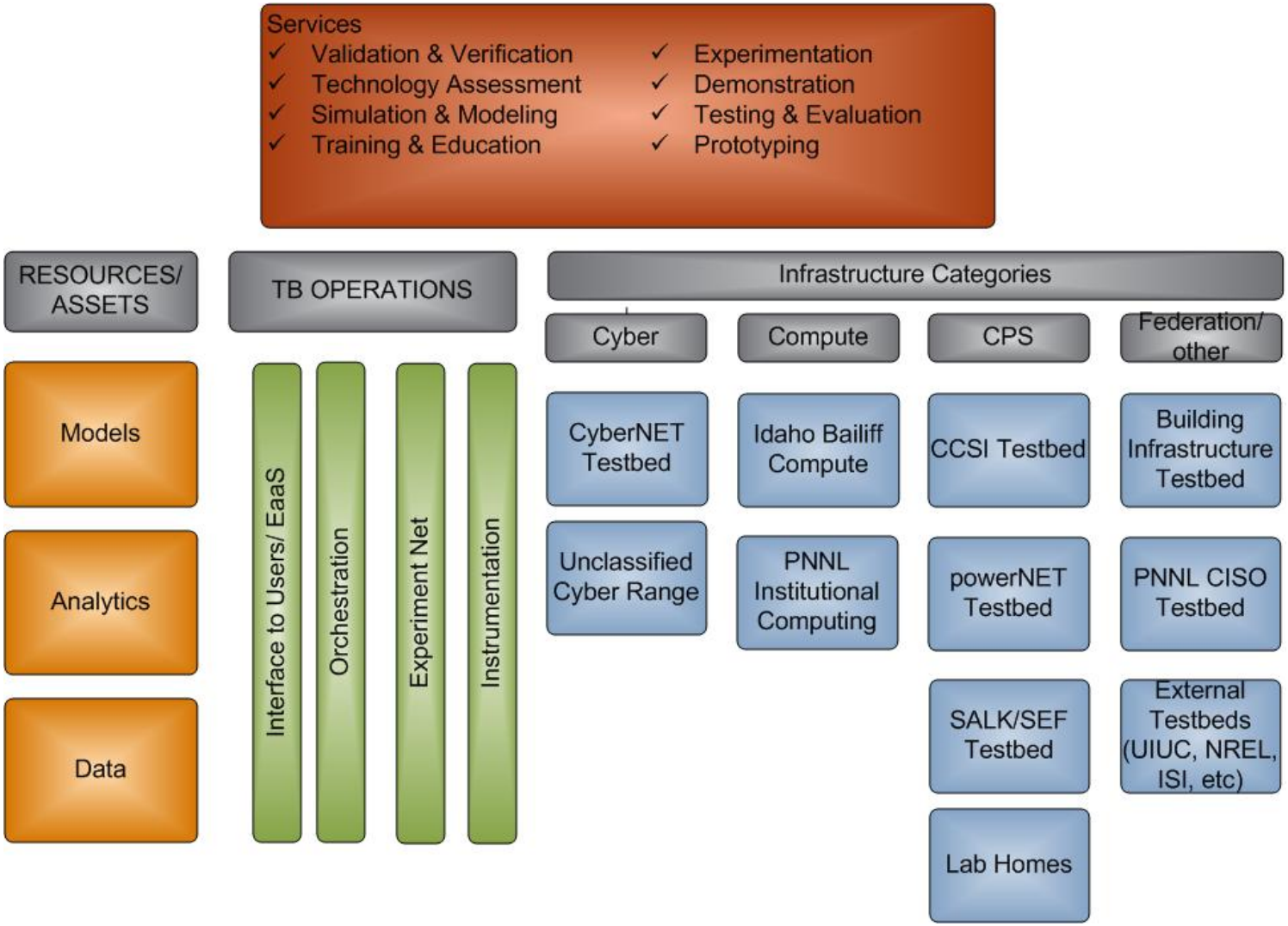
- Increasing scrutiny and threat
- Large amounts of functionality upgrades
  - Deployments without adequate investigation
- High resource requirement
  - Expensive equipment
  - High knowledge/experience barrier to configure and maintain
- Lack of access to equipment by researchers
- Experimentation can not occur in operational environments

Vision for a Testbed

- Experiment-based
  - Fidelity and repeatability
    - Simulated environments
    - Low-level access to equipment
- Scalable
  - Emulation and simulation
- Dynamic and flexible
  - User-friendly
  - Common library of scenario templates
  - Reset to known between configurations
- Multi-user capability
  - Experiment and data separation
  - Access controls
- Modular and expandable
  - Capable of federation
- Self supported user community

Research Infrastructure @PNNL: Holistic view

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

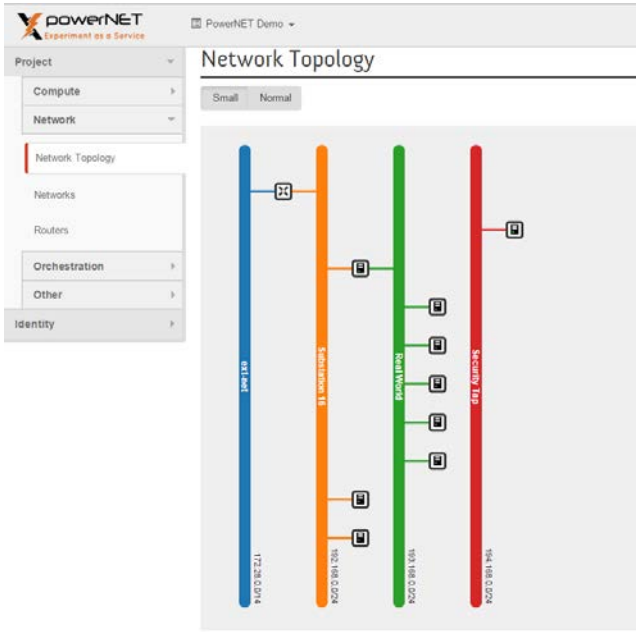


PNNL powerNET Facilities

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle *Since 1965*

- **Cloud technology based orchestration with web based user portal**
- **Network Emulation**
  - Emulate LAN/WAN communication characteristics.

  Examples:
    - Dedicated Line
    - Dial-up
    - Wireless
- **SCADA environments**
  - Real equipment to model ~two substations
    - ABB, GE, Siemens, SEL, …
  - Software simulation of dozens of SCADA equipment
  - Support for legacy communications



powerNET
Experiment as a Service

powerNET Facilities (cont.)

- **Physical Process Emulation**
  - Hardware-in-the-loop modeling
  - Opal-RT
  - Large scale simulation
- **Synchrophasors**
  - 9 PMUs from variety of vendors
    - 1 PMU Development Platform
  - 1 Hardware PDC
    - (Many software PDCs possible)
- **Up to ~1000 general purpose virtual nodes possible**
  - XenServer hypervisor
- **Energy Management System**
  - **Alstom System**

PNNL cyberNET Facilities

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Facility investment by PNNL
  - Scientific experimentation
  - Real-world scenarios
  - Cyber security metrics

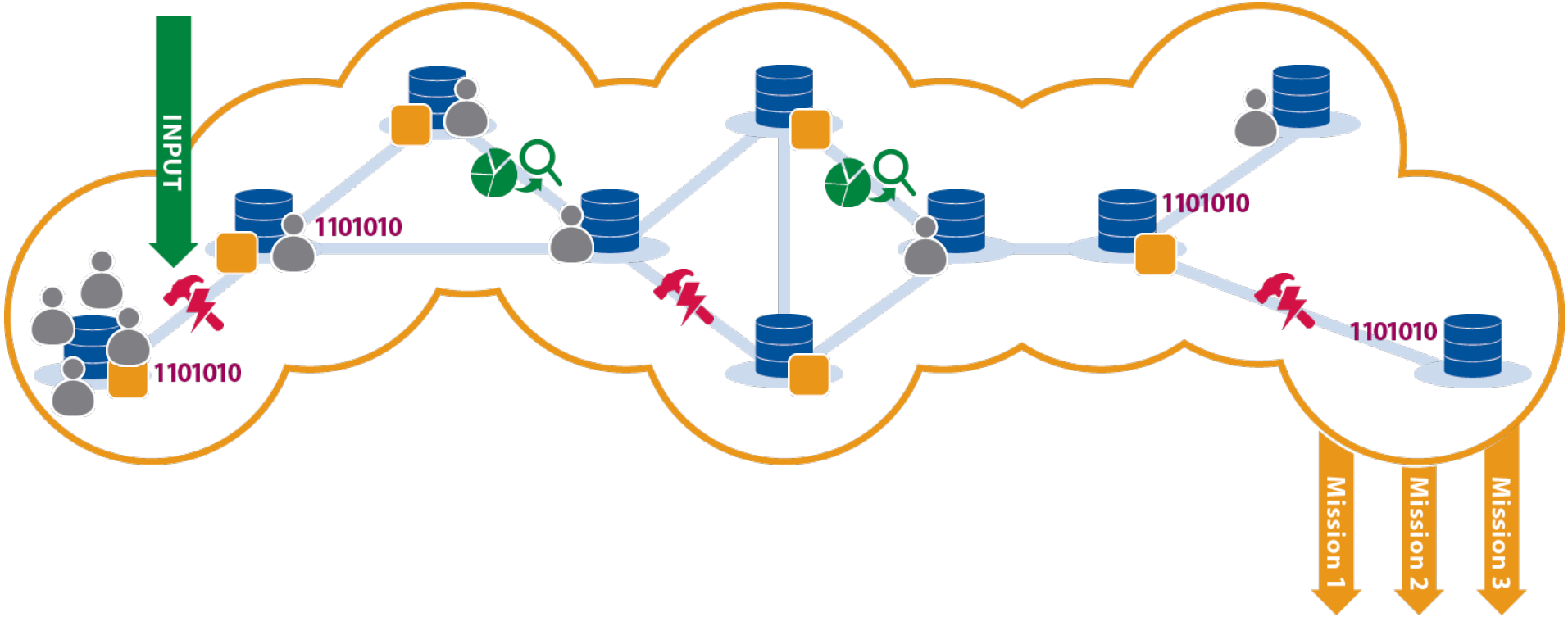
- Leverages:
  - Commodity hardware
  - Commercial and open source software
    - Citrix XenServer, OpenStack
    - Agent platform for user emulation
  - PNNL modifications for science
    - Repeatability, sensoring, control…

cyberNET
Experiment as a Service

cyberNET Facilities (cont.)

- Combination of simulation, virtualization, and real equipment
- Repository for storage/retrieval of experiment data
  - 120TB
  - Support development of "gold standard" test datasets
- Multi-user/multi-project support
  - Share resources
  - Quick setup/configuration
- Simulates up to ~4000 virtual nodes
  - Currently 28 nodes (32 core, 256GB)

ViSR Company



System | Network | ViSR | Application | User | 1101010 Data | Actuation | Sensing

Testbed Uses

- Technology assessment and prototyping
- Simulation and modeling, verification, and validation
- Experimentation
- Demonstration
- Training and education

Cyber Security Science Contributions

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Testbeds for rigorous experimentation
  - Multi-user shared facility and equipment
  - Time and resource efficient
  - Dynamically configurable
  - Federatable to a larger user community
- Measurable science
  - Understanding and creation of gold standard data sets
  - Rigorous approach (repeatability, system under test, appropriate fidelity, etc.)
- Improved awareness through training and exercises

Cyber Science & Community Challenges

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Accuracy of system
  - Scale
  - Fidelity
  - M&O (staleness)
- Accuracy of humans (cyber)
  - Blue team automation
  - Red team automation
  - Human red team utilization (sample size, learning, uniformity, access)
- Reproducibility
  - Who does it?
  - Who pays for it?
  - How do we facilitate it?

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

David Manz
Principal Investigator
CyberNET Testbed

david.manz@pnnl.gov

Asymmetric Resilient
Cybersecurity Initiative

cybersecurity.pnnl.gov