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

# Cyber Security Resiliency: Measuring the Myth & the Mission

DAVID MANZ, PHD

Pacific Northwest National Laboratory

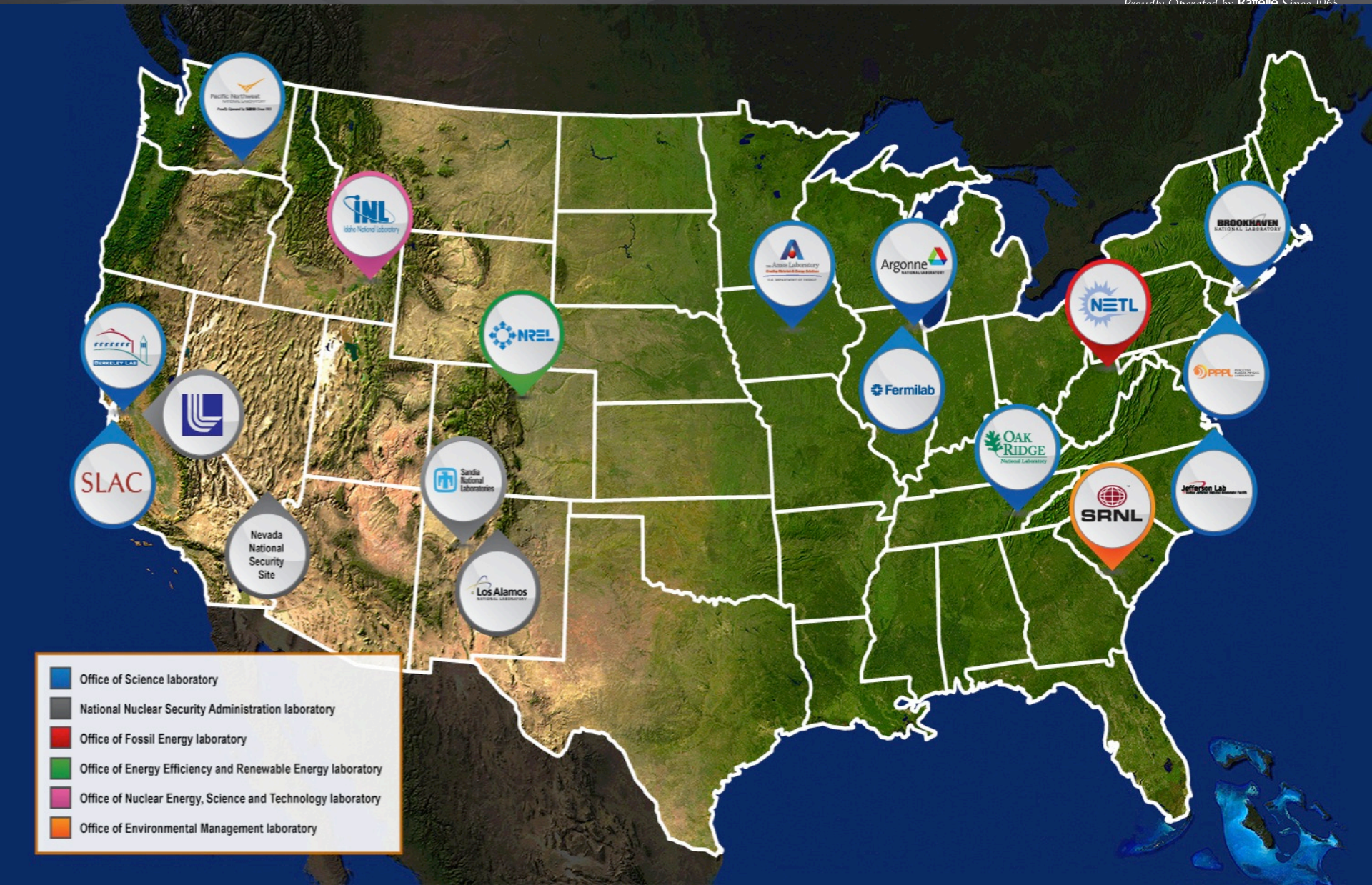
Presentation to the University of Idaho Computer Science Colloquia March 2017

U.S. DEPARTMENT OF
ENERGY

# DOE's Laboratory System is Solving America's Toughest Challenges

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965



# PNNL leverages its science base to provide national leadership

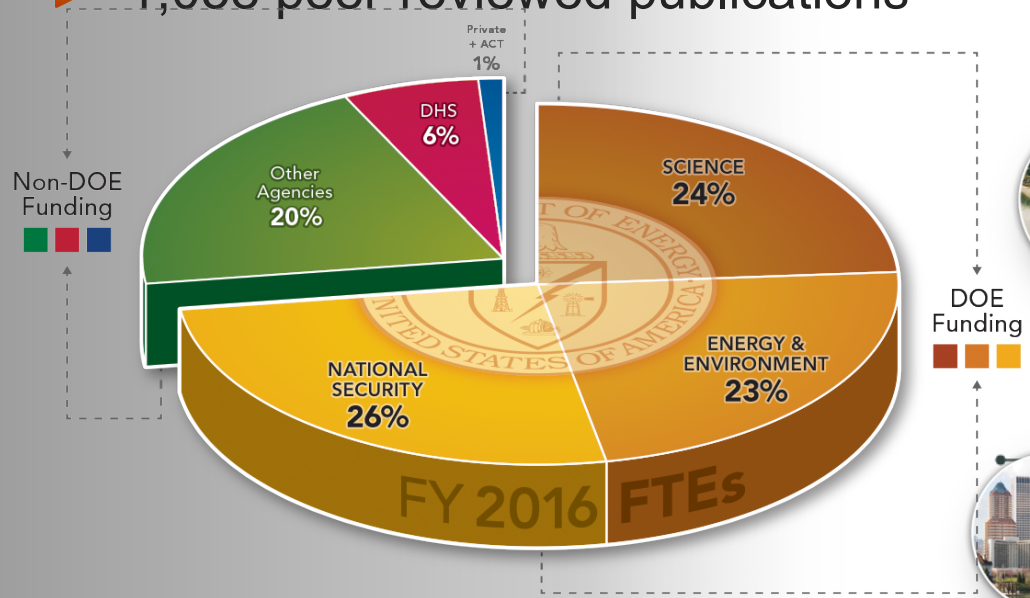
Pacific Northwest
NATIONAL LABORATORY
*Proudly Operated by* Battelle *Since 1965*

# PNNL – FY2016 at a Glance

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

- $920.4M in R&D expenditures
- 4,400 scientists, engineers and non-technical staff
- 104 U.S. & foreign patents granted
- 2 FLC Awards, 2 R&D 100
- 1,058 peer-reviewed publications

- Mission-driven collaborations with government, academia and industry
- Among DOE's top-performing labs; a premier chemistry, environmental sciences and data analytics laboratory




# PNNL's Computing Capabilities

## Mission-Focused Technology Development

Pacific Northwest NATIONAL LABORATORY

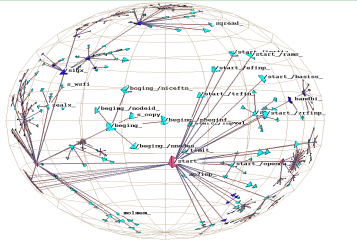
*Proudly Operated by* Battelle *Since 1965*

### COMPUTING ENVIRONMENTS

- High Performance Computing
- Quantum information science
- Large-scale data management
- Mobile and edge computing
- Embedded systems
- Cloud and streaming architectures

### ANALYTICS

- Discrete mathematics and graph theory
- Human language technology
- Image processing
- Machine learning and recommender engines
- Social, behavioral science



### DECISION SUPPORT

- Information visualization
- Human-computer interaction
- Virtual and augmented reality
- Analytic tradecraft and critical thinking
- Collaboration systems


### MISSION APPLICATIONS

Cyber-Physical Systems | Biosurveillance | Social media | Forensics | Emergency preparedness and response | Biostatistics, proteomics, climate | Power grid management | Critical infrastructure resiliency | Trafficking

# PNNL's Cyber Portfolio

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


- Cyber Security Research
- Cyber Security Operations
- Applied Cyber Security Solutions
- Cyber Analytics

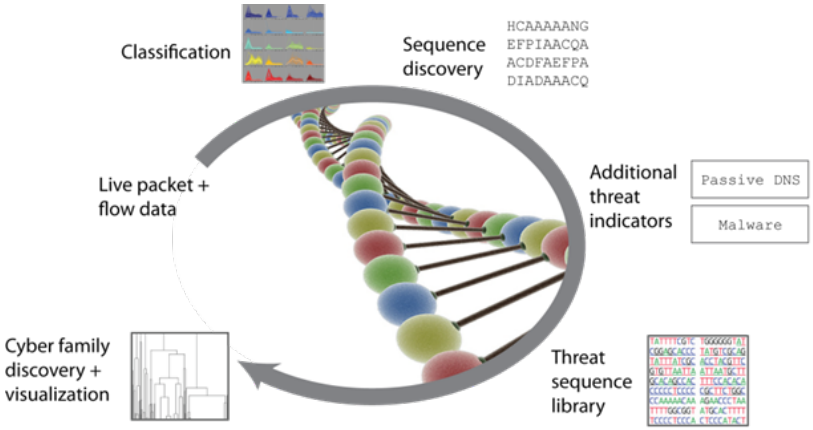
# Cyber Security Research

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

- Advancing and Formalizing the Science of Cyber Security
  - Experimentation and scientific methodology
  - Testbeds: cyberNET, powerNET
    - Dynamically reconfigurable and remotely accessible experimental environments for research, education/training, and commercial interoperability testing
    - Power, oil and gas, water, healthcare systems
  - Datasets
- Bio-inspired hypotheses
  - Digital Ants
  - MLSTONES
- Internal investments
  - Asymmetric Resilient Cybersecurity

cyberNET
Experiment as a Service

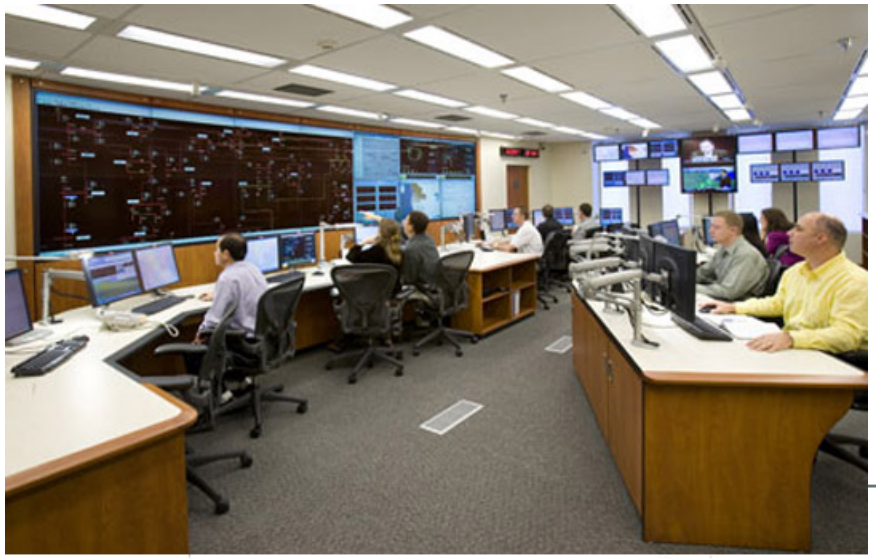
powerNET
Experiment as a Service



# Cyber Security Operations

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

- Cyber Network Defense
  - Partnership between Research and Operations
- Cyber Situational Awareness Systems
  - Cooperative Protection Program
  - Cyber Risk Information Sharing Program



CPP
COOPERATIVE PROTECTION PROGRAM

# Securing Critical Infrastructure

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

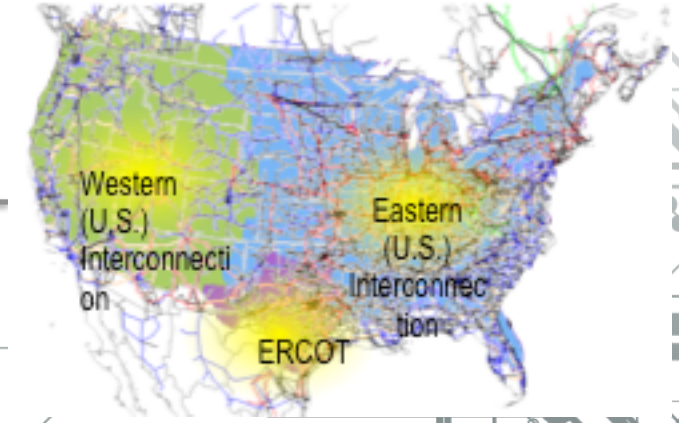
## CHALLENGE

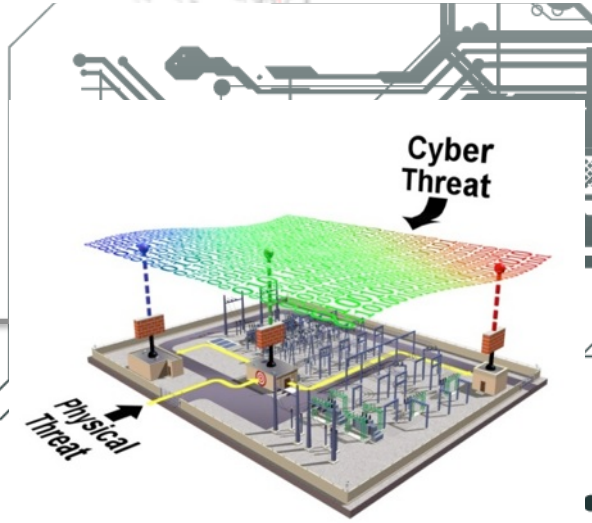
A safe and reliable energy grid and network of industrial control systems requires new approaches to secure information sharing and prevention of cascading failures.

## PNNL APPROACH

Wide-area situational awareness capabilities for critical infrastructures enable real-time operational response to active cyber threats.

PACRAT cyber-physical security programs include vulnerability assessments for SCADA and other control systems and secure control system protocols.



# Component Security & Hardware Characterization

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

## CHALLENGE

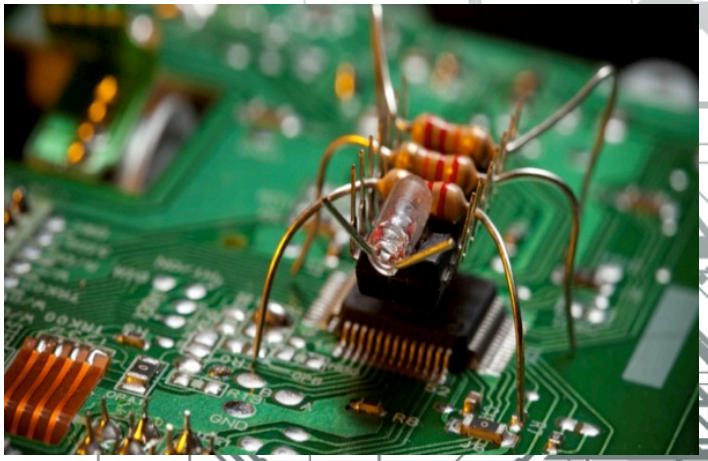
Ensure the integrity of mission-critical computer hardware and firmware components across the global supply chain.

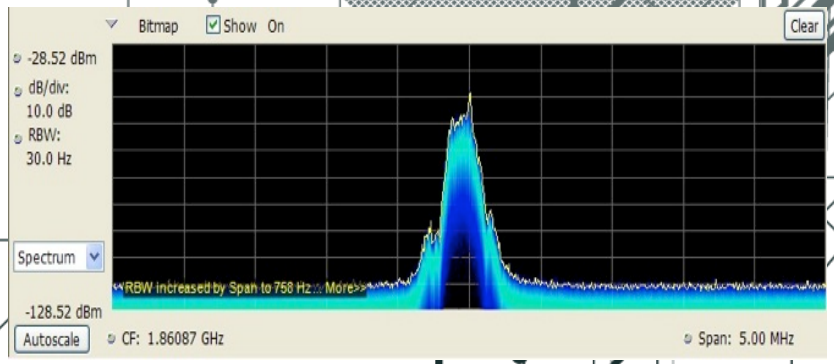
## PNNL APPROACH

Specialized diagnostic and monitoring tools enable Identification of malicious code injection and pirated hardware.

Fingerprint mobile devices in crowded EM environment by exploiting artifacts in transmitted or emitted RF due to variability in device components.

Hardware-based CPU instruction set encryption prevents unauthorized code execution & creates unique devices to eliminate computing monoculture; minimally impacts performance, suited for embedded devices.





# Cyber Analytics

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

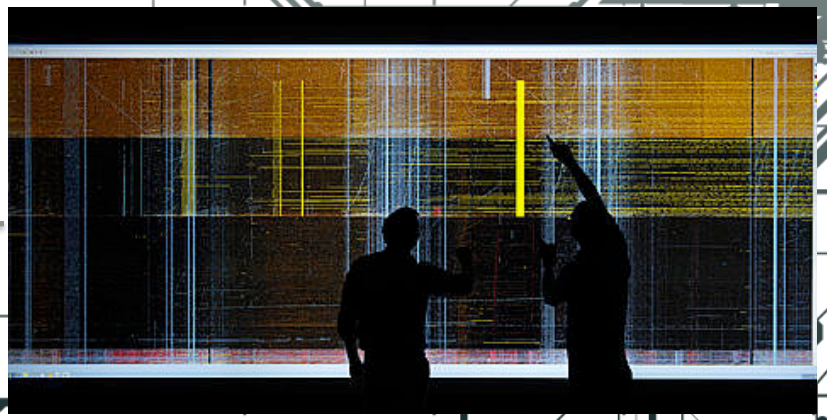
## CHALLENGE

Online threats evolve rapidly and are hidden in mass
performance data processing and anomaly detectior

## PNNL APPROACH

PNNL's behavior modeling algorithms and bio-inspired string matching have been used to search evidence of cyber compromise and malware.

A scalable visualization system for computer network communications helps analysts discover suspicious transactions.

# PNNL's cyber strategy will drive and enable a strategic national approach

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- The defining security challenge of our time
- A key role for national labs
- A mandate for PNNL leadership
- Elevated PNNL leadership and substantial mission impact

## SHAPE THE EMERGING CYBER BATTLEFIELD

- Reveal adversary strategy and tactics
- Counter adversary strategy and tactics at PNNL
- Control high-consequence systems

# Cyber Security Problems Today

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Attribution
  - May not be an issue for you
- "Provable" security
  - Effectiveness
  - Measurability
  - Lifespan (silver bullet)
- Developing relevant security
  - Security in context
- Problem exists between chair and keyboard
  - Is the user to blame (phishing, watering hole, plugging in USB drives)?
  - Is the developer to blame?
  - What is the role of the human as a user and defender?
- Reliability vs. safety vs. security vs. resilience

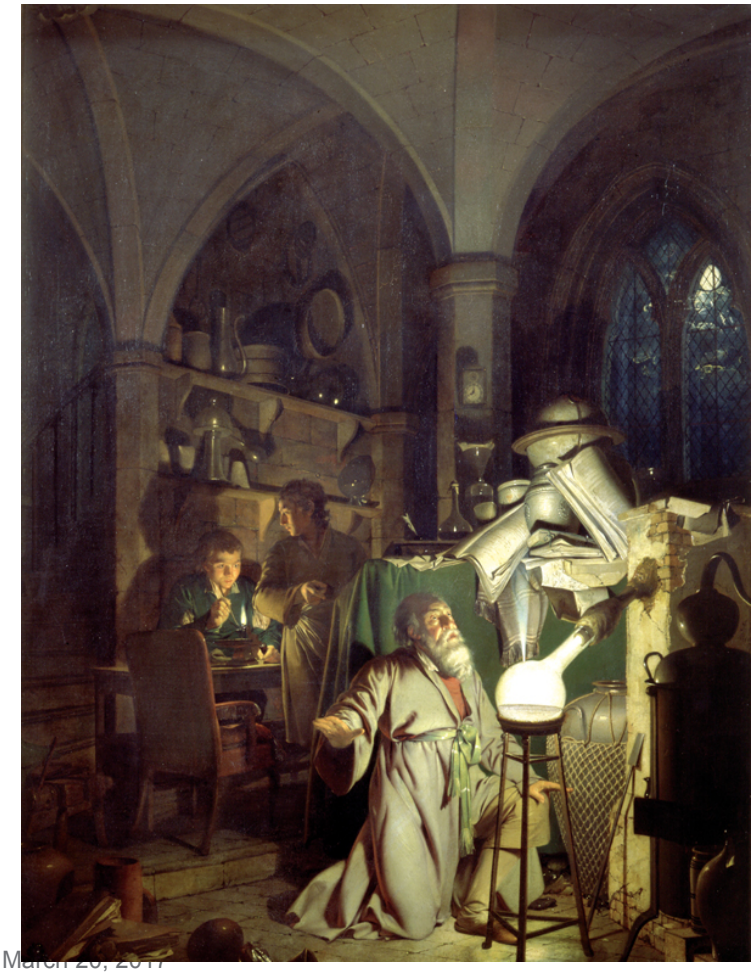
# Science of Cyber Security

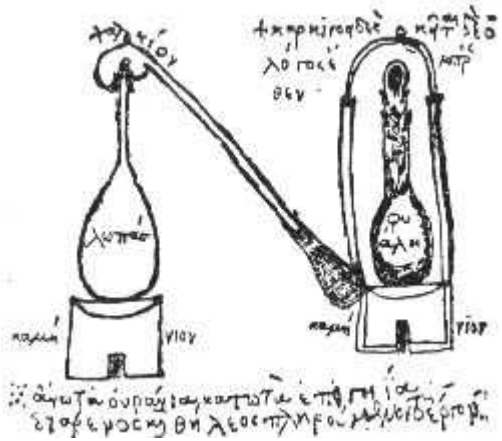
Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Problem
  - Treating as applied science without fundamental science foundation
- Approach
  - Methods for performing rigorous scientific research
  - Theories for the field to begin building a body of knowledge
  - Review field for successful research
- Impact
  - Move toward resilience for defender
  - Enable metrics – ability to measure
  - Support decision making

# Cyber Security Science & Alchemy

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





# Cyber Security Science & Alchemy

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Transmute lead into Gold

$_{82}Pb \rightarrow {}_{79}Au$

- Define mathematical laws for cyber phenomenology

# Path Forward

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

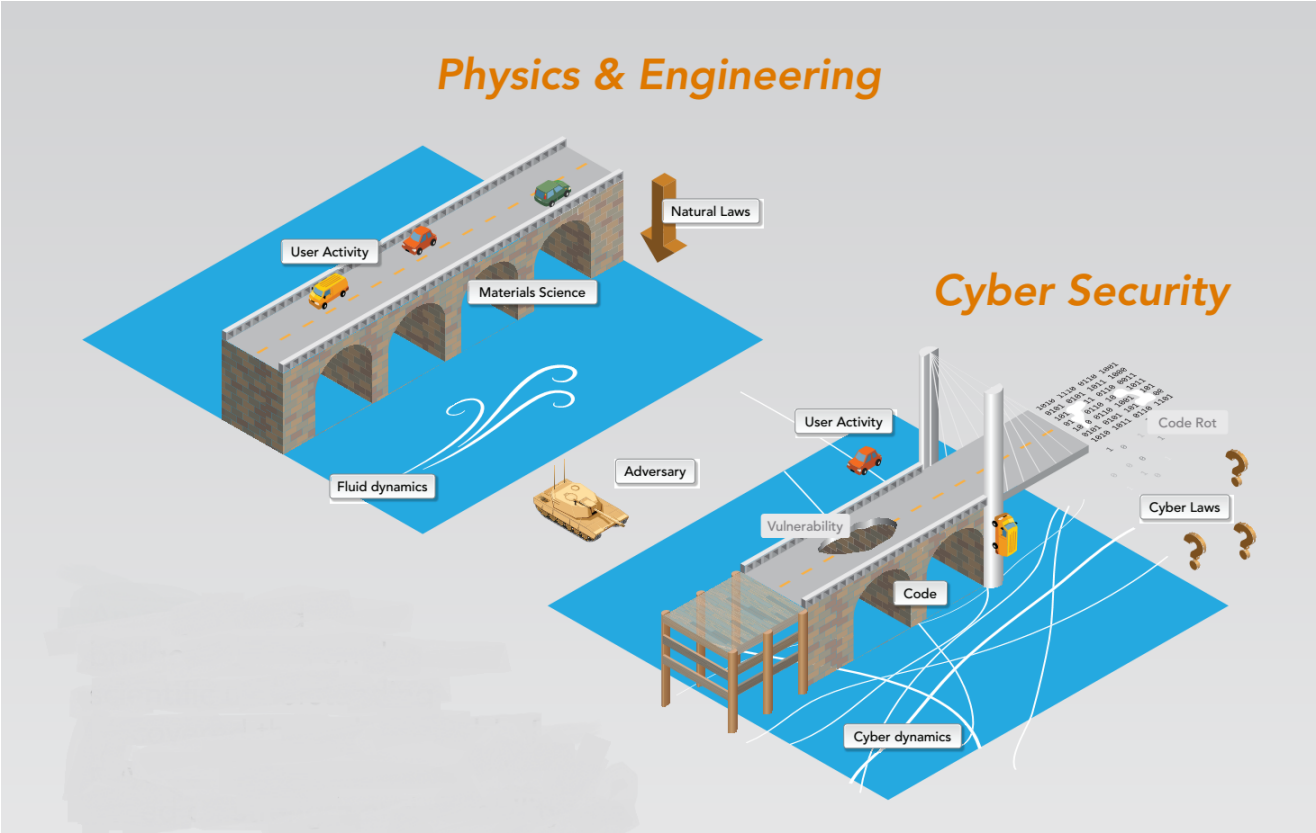
- Best practices are necessary but not sufficient
  - See Verizon, Symantec, Mandiant, FBI, Tofino, GTRI, etc. reports
- Gain understanding
  - Of our own domain
  - Of the adversary
- Develop validatable and quantitative defenses and options for defender

Premise: This requires science

# What Does Science Provide?

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

- Experimentation
  - Models/simulation
    - Biological examples
  - Testbeds
- Evidence
  - Repeatable
  - Reproducible
  - Falsifiable
  - Controlled biases
- Observation
  - Describe future behavior
  - Provide assurance



# Attributes of cyber science: Scientific questions

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

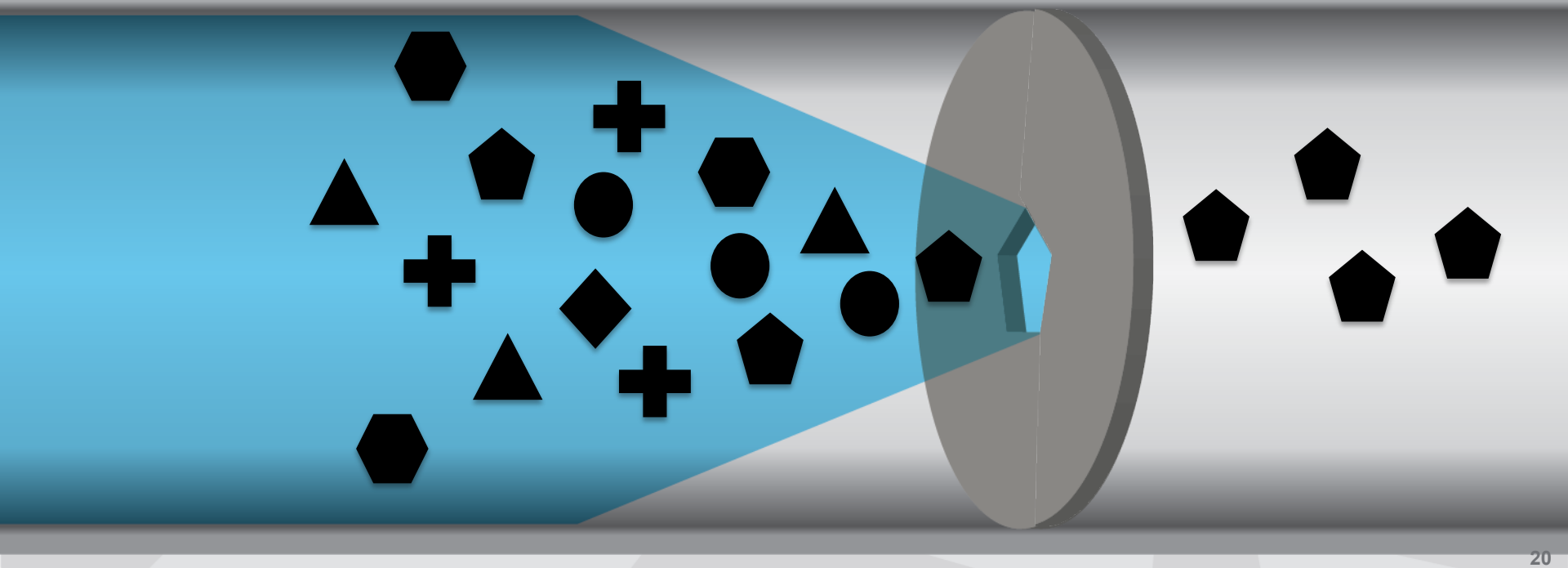
- Mechanics
  - Understanding the how and what of cyber space
  - Discrete vs continuous system modelling
  - Contextual specificity (dimensionality, ordinality, identity, speed)
- Measurements
  - Sensemaking (ascribing meaning)
  - Exploring exogenous and endogenous sensors (what is observable)
  - Significant units
- Cyber-Social Phenomenology
  - HCI
  - Techno-social cognition
  - Adversarial coevolution & competition
- Predictions (culmination)
  - Actuarial evidence
  - Cyber Forcasting (weather)
  - Quantifiable Cyber Risk

# What is Resilience?

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

**Resilience:** The degree to which a cyber system will continue to support mission in the face of impediments

**Resilience: Characteristic of a system**



# What do we measure

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Take a medium sized business that manufactures power control equipment
- Workstation “health” / security
  - Antivirus/ malware
- Network activity
  - IDS – detection
  - Firewalls -prevention
- Servers
  - SIEM
  - System Logs
- O.T.
  - Manufacturing plant

# Classic Information Assurance



- CIA
  - Confidentiality
  - Integrity
  - Availability
- Others could include auditing, authenticity, accountability, trustworthiness, non-repudiation, and privacy.

# Availability Measures?

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Redundancy
- Diversity
- Functionality
- Restoration
- Honestly/ Trustworthiness
- Connected/ Open
- Deterministic
- Coordinated

# Integrity Measures?



- reduced complexity
- simplicity (i.e. code)
- deflect (i.e. honey pot vs. firewall)
- Dynamic (moving target)
- Absorb

# Confidentiality Measures?

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- reduced attack surface
- deflect (i.e. honey pot vs. firewall)
- Dynamic (moving target)
- Deception
- Segmented/ Restricted
- Unpredictable
- Autonomous

# Other security measures

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- situational awareness
- forensic analysis
- Impact
- Cost
- Reserve Capacity (shields)
- sacrifice (retreating defense)

# What about the mission/ business

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

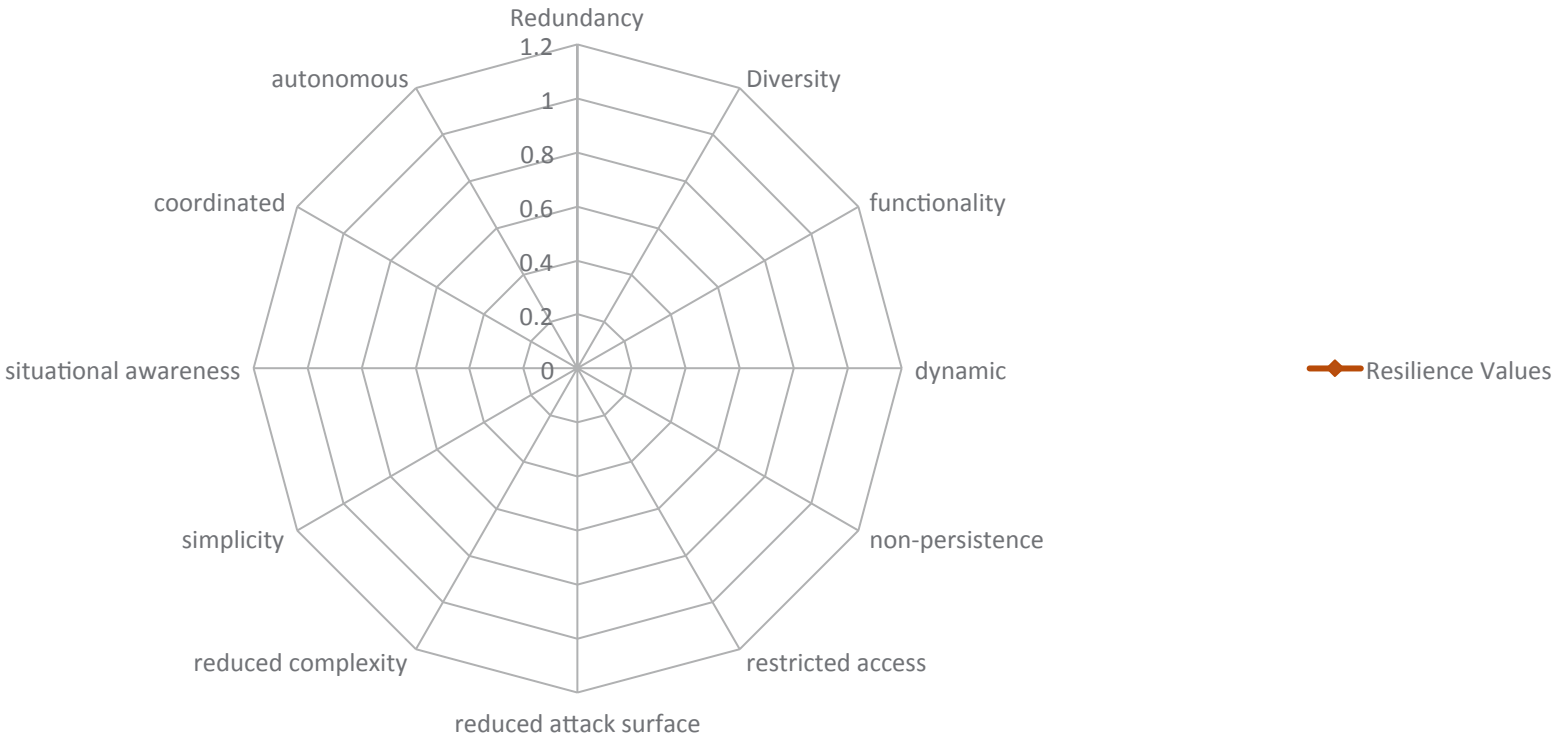
- Continuity of Business CooB / operations/ planning/ missions/ government
  - Continues to perform essential functions
  - Sounds like resilience?
- How do you map from computer/ network to business
  - Assets
  - security

# Human element

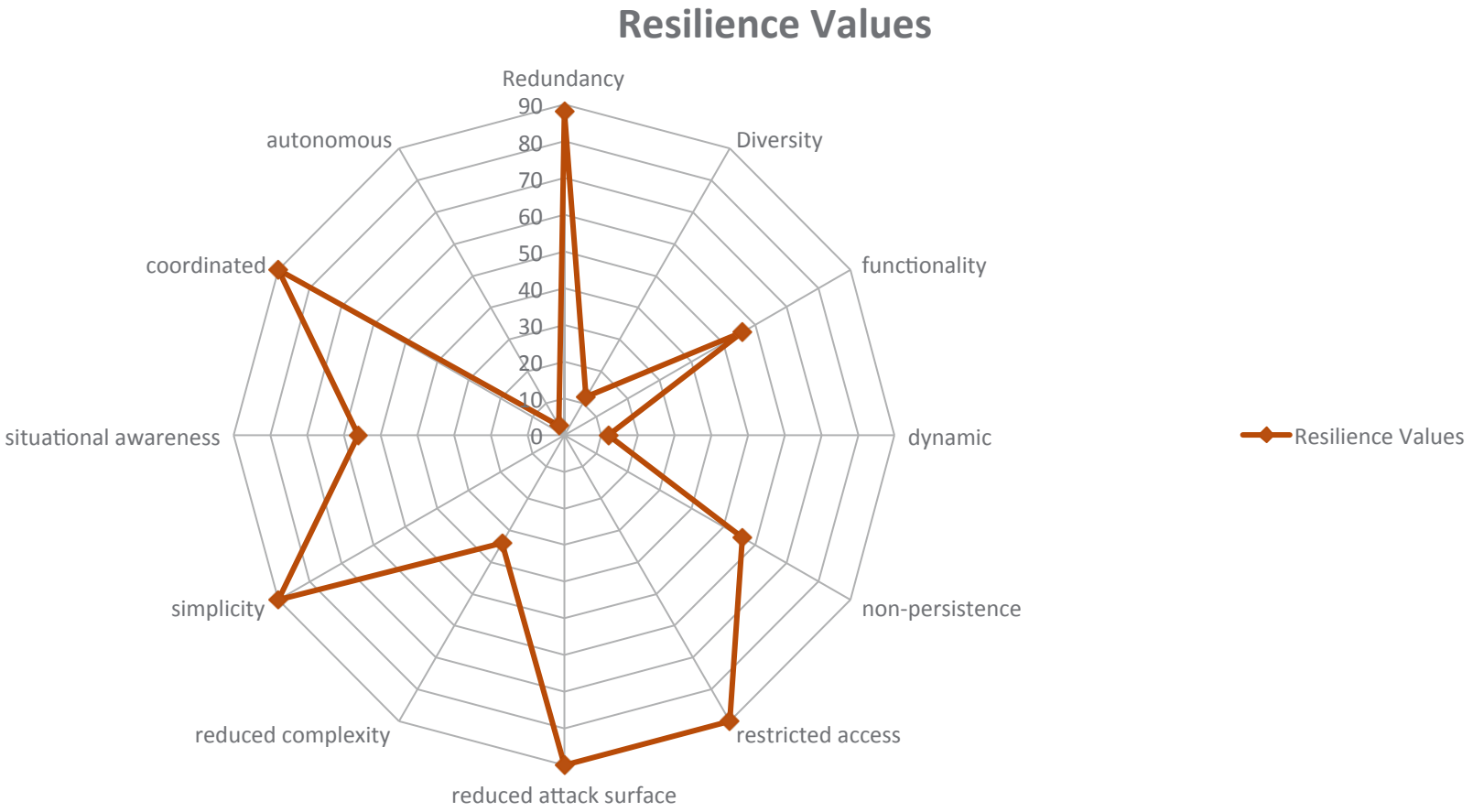


- Insider threat
- Espionage
- Theft
- Vandalism
- Activism

# Resilience Values



# Per Attack


Resilience Values
Redundancy
Diversity
functionality
dynamic
non-persistence
restricted access
reduced attack surface
reduced complexity
simplicity
situational awareness
coordinated
autonomous
90
80
70
60
50
40
30
20
10
0
Resilience Values

# Cyber Risk

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

- Like any other risk
- **Risk** is the probability of an event occurring in the context of the:
  - Asset being protected
  - Abilities of the adversary
  - Vulnerabilities that can be exploited
  - Harm that can be inflicted
- Or is it?
  - $R \neq T \bullet V \bullet C$
  - Calculating risk is not static

# Cyber resilience



- Which is cyber enabled mission resilience
- Which is a spider graph per attack, constantly updating per system

# PNNL Capabilities

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Discover fundamental science to improve effectiveness of technology
- Develop and evaluate new defensive solutions
- Transition technology for commercialization
- Educate on issues and forthcoming R&D
- Applied to:
  - Cyber Analytics
  - Component Security
  - Control Systems Security
  - Resilient Cyber Security

# Questions?

Contact information:
**David Manz, Ph.D.**
(509) 372-5995
david@pnnl.gov