Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Asymmetric Cyber Resiliency and Its Validation

NICK MULTARI, PH.D
ASYMMETRIC RESILIENT CYBERSECURITY INITIATIVE
PACIFIC NORTHWEST NATIONAL LABORATORY

January 27,2017

Approved for public release
PNNL-SA-121482

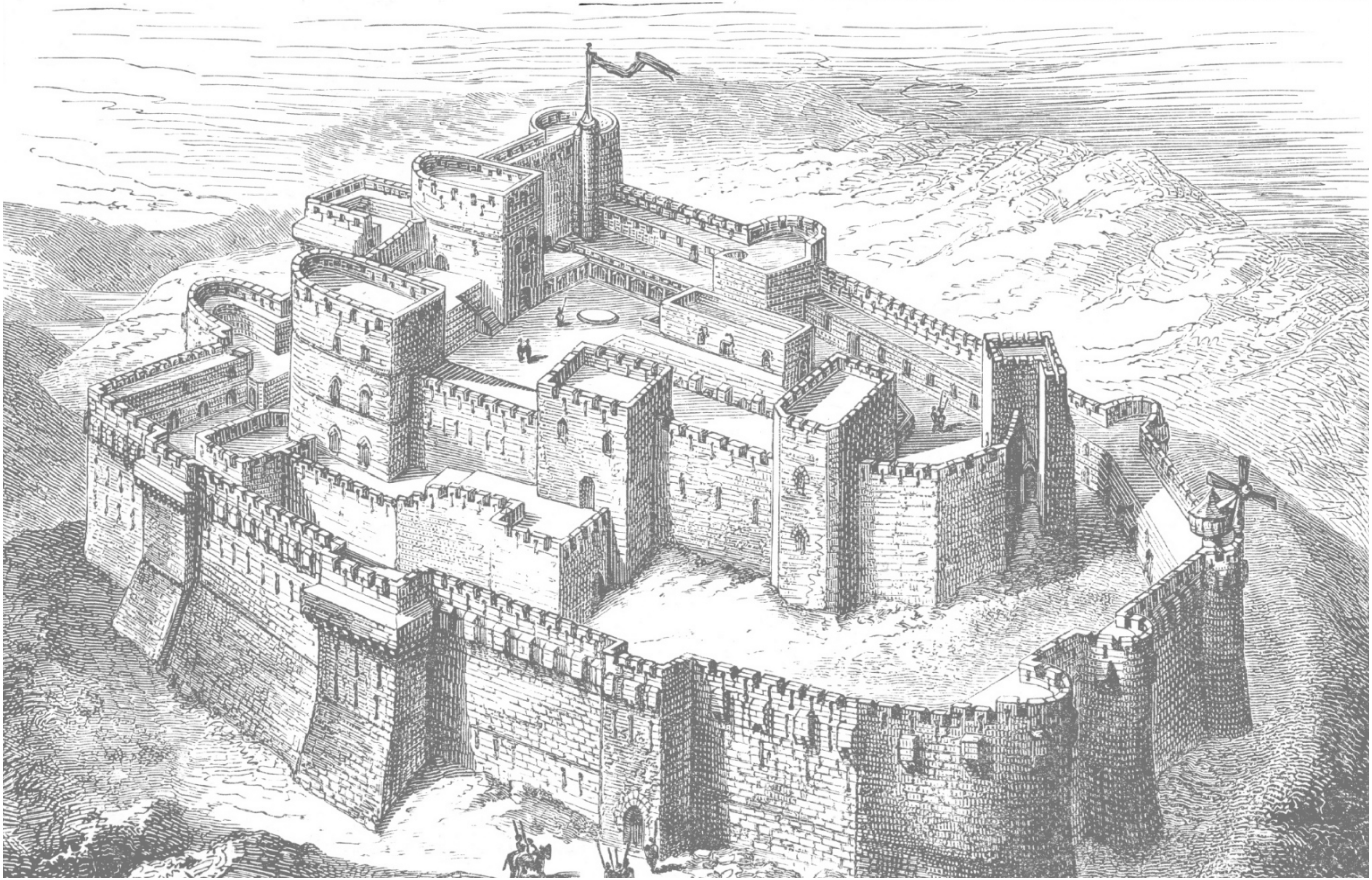
Asymmetry in the Beginning

… then the defender reacts

Today’s Cyber Challenge

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*



PNNL's Asymmetric Resilient Cybersecurity Initiative Concept

Deliver the theory, processes, methodologies, and algorithms that will enable a **resilient cyber infrastructure** with an **asymmetric advantage**, thwarting adversaries who seek to infiltrate and damage our national security through digital means

So what needs to happen next?

- Define what we mean by asymmetry
- Create platform to make measurements
  - Understand bias, errors introduced by this platform
- Obtain candidate technologies to be evaluated
- Make repeated experiments
- Evaluate results

Definitions of Asymmetry

Asymmetry is not an intrinsic property:

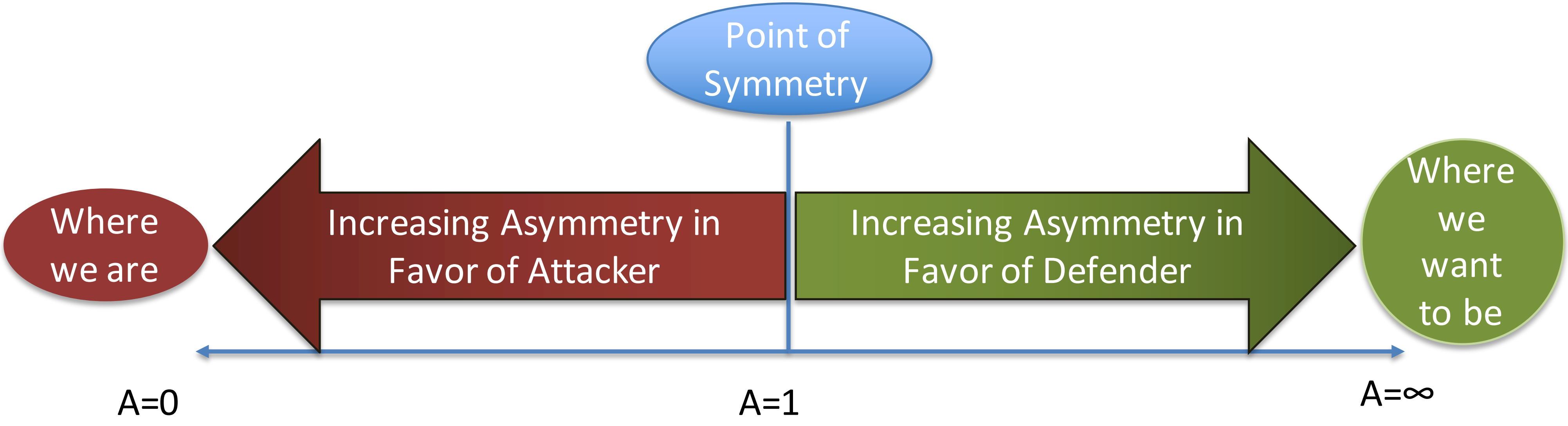
You have to specify something about the entities engaged in a conflict for asymmetry to make sense.

- Disproportionate, exploitable imbalance between competing parties
- Asymmetry can be applied to
  - Threat-
    - Small organization with modest resources becoming a threat to a large organization
    - Large organization with generous resources threatening a medium-to-small organization
  - Action- low cost defensive measures foiling high cost measures
- A quality that creates imbalance between actors in the resources, level of effort, risk, or consequences in an attack

Asymmetry as a Scalar

Let's explore a definition of Asymmetry as Attacker Cost/Defender Cost:

$$A=C_a/C_d$$


Point of Symmetry
Where we are
Increasing Asymmetry in Favor of Attacker
Increasing Asymmetry in Favor of Defender
Where we want to be
A=0
A=1
A=∞

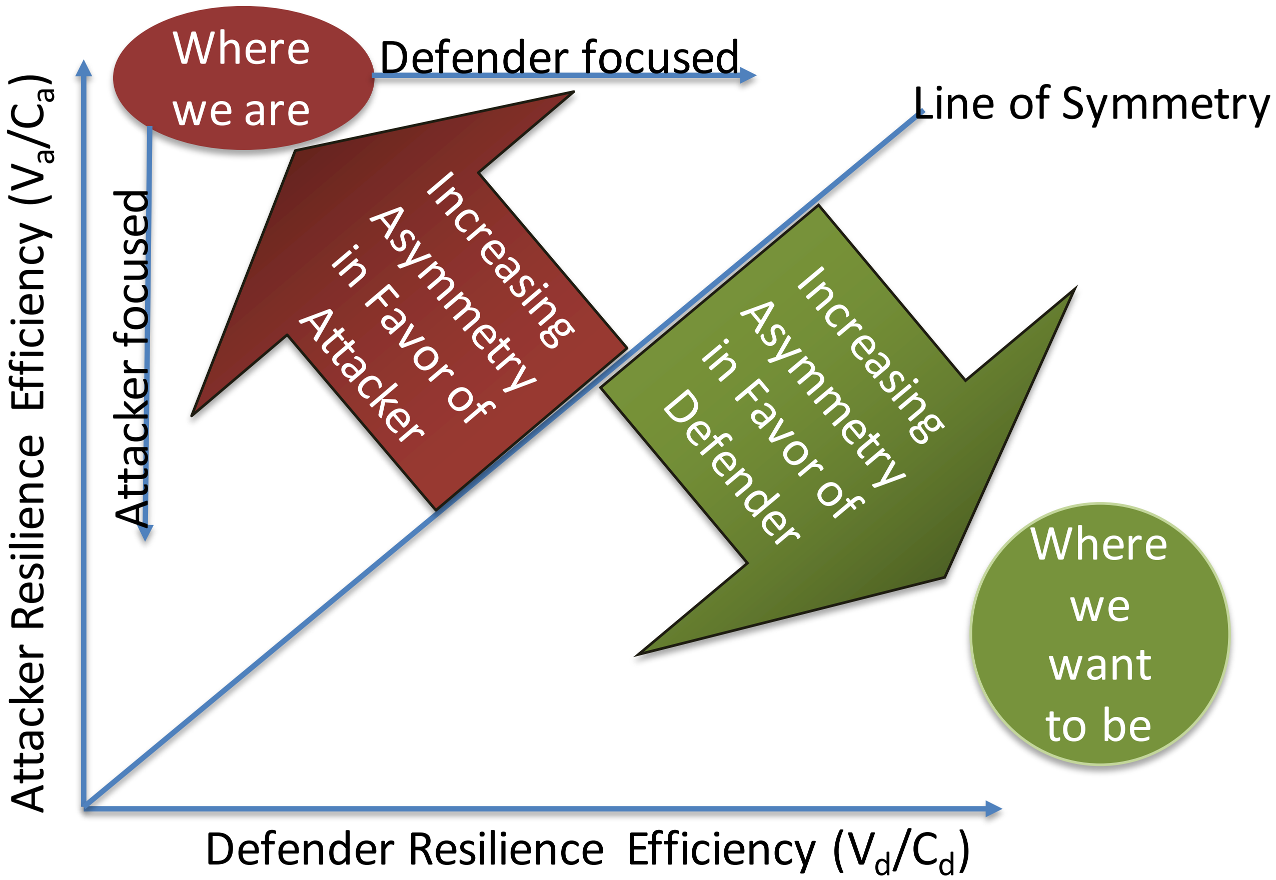
Cost = \$, effort, time, risk, inconvenience, **impact to mission**, …
Might make sense if we are similarly resourced, but how often is this reasonable?

Asymmetry as a Vector

Now consider Asymmetry as a vector of two quantities, each measuring relative resilience value and cost for either attacker or defender:

$$A=(V_d/C_d,\ V_a/C_a)$$

$$\mathbf{V_a \neq V_d}$$


Where we are
Defender focused
Line of Symmetry
Attacker focused
Increasing Asymmetry in Favor of Attacker
Increasing Asymmetry in Favor of Defender
Where we want to be
Attacker Resilience Efficiency (V_a/C_a)
Defender Resilience Efficiency (V_d/C_d)

So we could also manipulate the attacker's value!

What if Asymmetry is even higher dimension?

What quantities should be part of the vector?

What if cyber resilience itself contributed to the defender's perceived value?

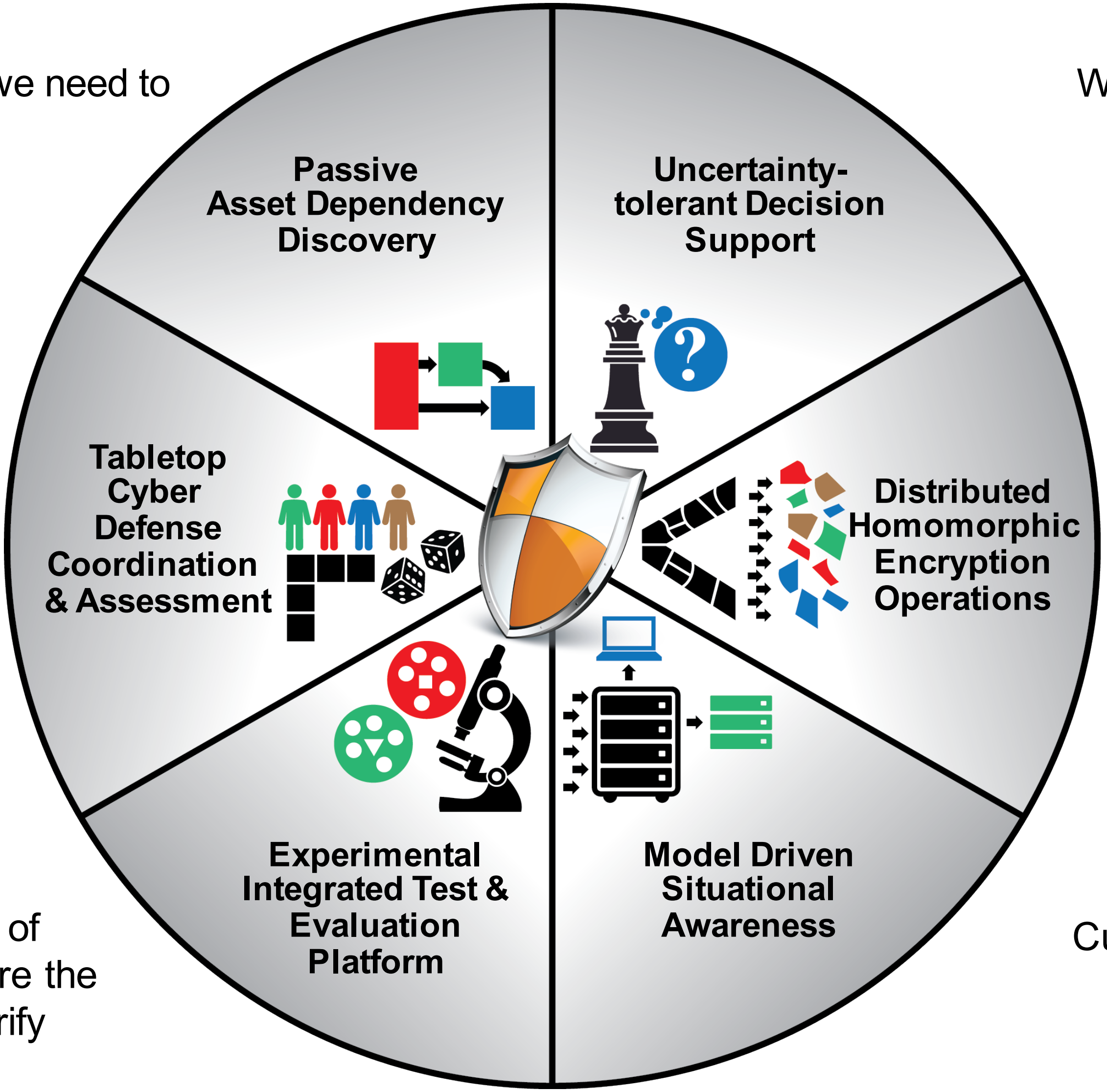
Addressing Key Gaps with ARC Capability Areas

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

Addressing specific technology gaps with novel R&D:

In dynamic systems, we need to track assets and their dependencies.

We will need to make good decisions with imperfect knowledge.


Passive Asset Dependency Discovery
Uncertainty-tolerant Decision Support
Distributed Homomorphic Encryption Operations
Model Driven Situational Awareness
Experimental Integrated Test & Evaluation Platform
Tabletop Cyber Defense Coordination & Assessment
?

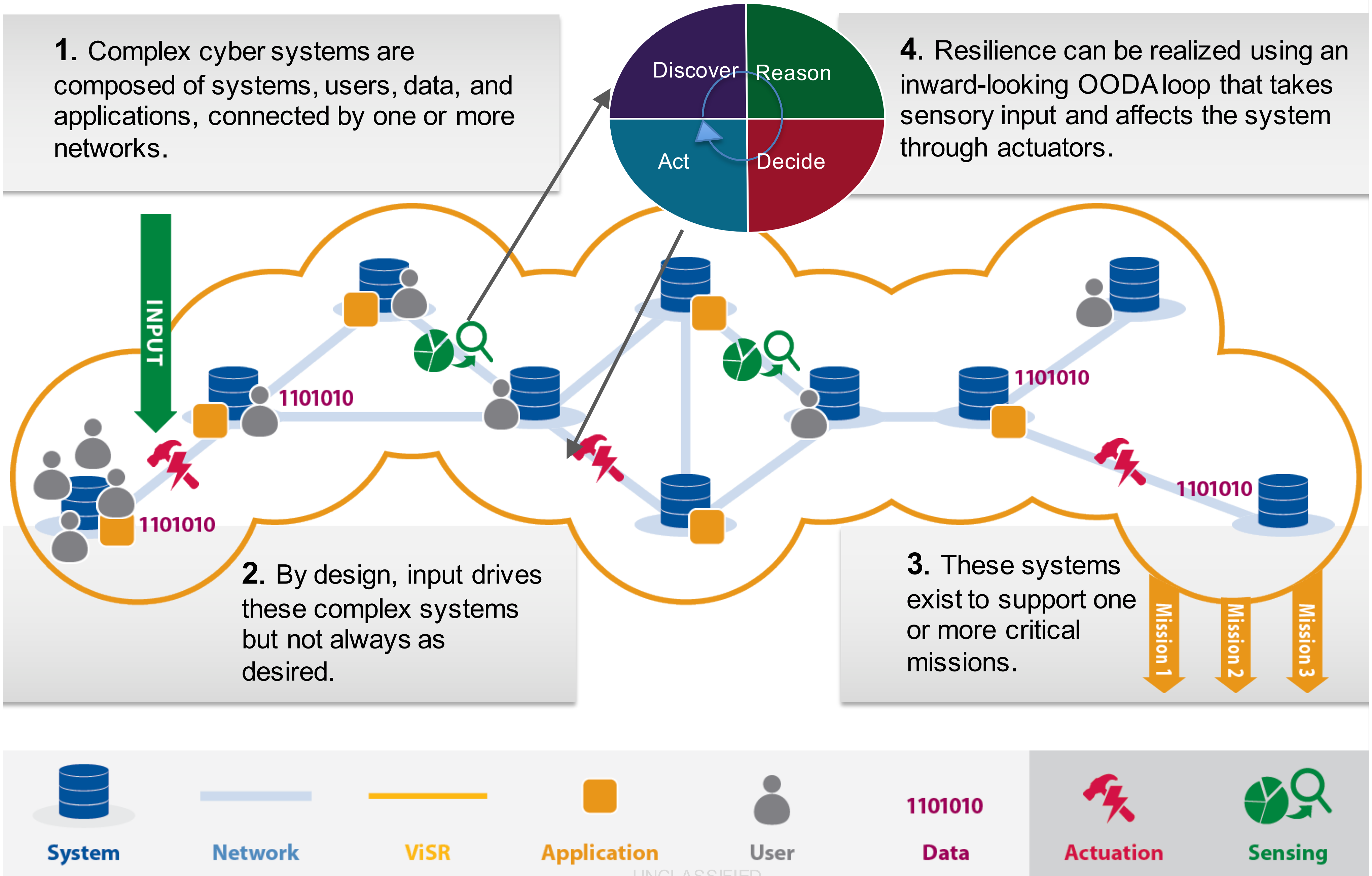
Resilience technologies will need to be usable by defenders.

Data at rest must be protected while enabling the range of operations that are necessary to make it useful.

Understanding impact of technologies will require the ability to rigorously verify performance.

Current sensors need to be supplemented with new information.

Vision: Resilient Cyber Systems



1. Complex cyber systems are composed of systems, users, data, and applications, connected by one or more networks.

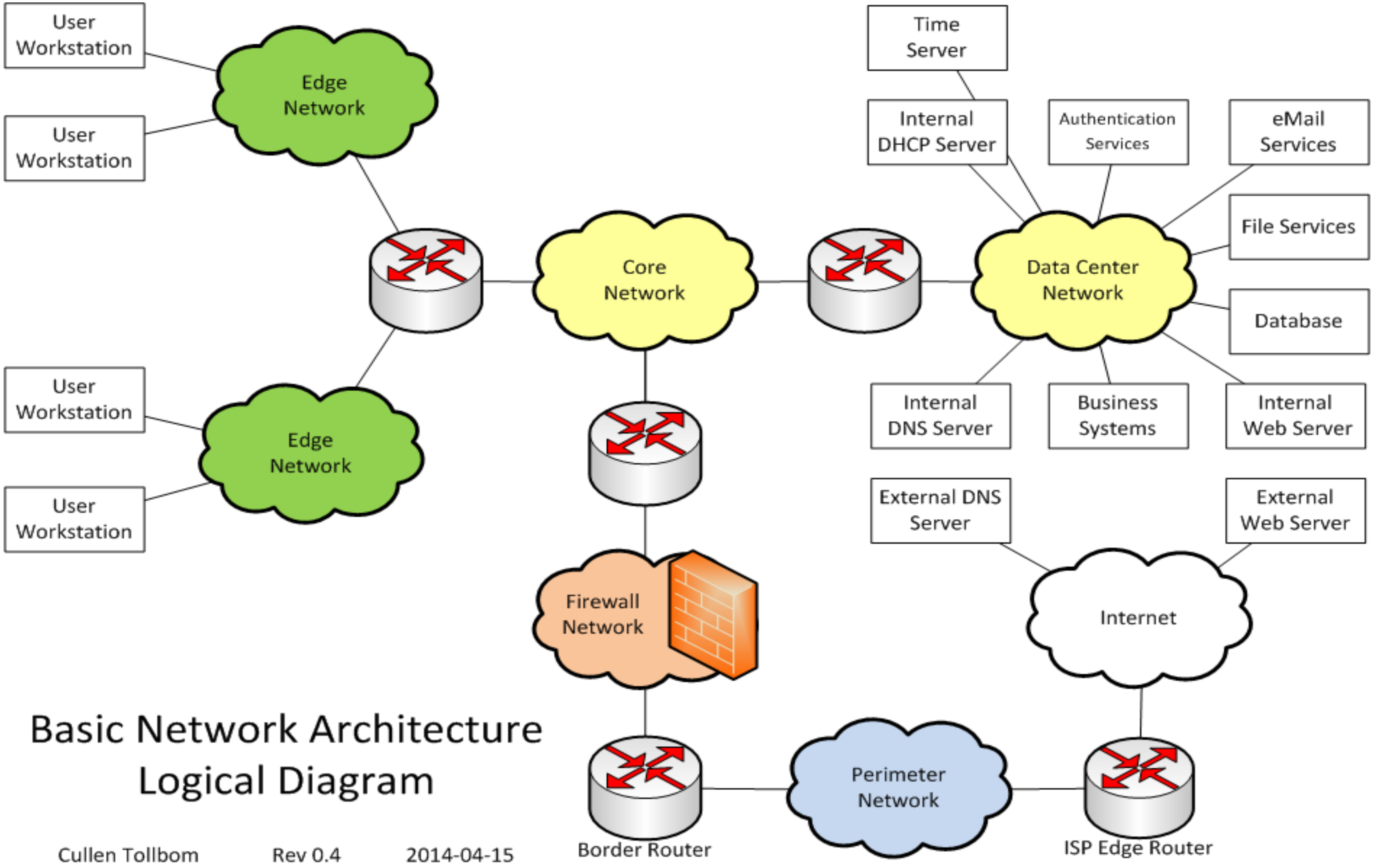
2. By design, input drives these complex systems but not always as desired.

3. These systems exist to support one or more critical missions.

4. Resilience can be realized using an inward-looking OODA loop that takes sensory input and affects the system through actuators.

Validation of Technology

Implementation of a Notional Company



Basic Network Architecture
Logical Diagram

Cullen Tollbom Rev 0.4 2014-04-15

Evaluating Cyber Security vs Cyber Resiliency

	Cyber Security	Cyber Resiliency
Objective	Defeat security mechanisms	Prevent critical function from executing
Assumption	Start from outside network	Start inside network
Means	Exploit vulnerabilities and the unexpected	Exploit vulnerabilities and the unexpected
Attacker success criteria	"Flag is planted"	Critical function execution prevented over a given timeframe
Defender success criteria	Keep adversary out	Mission persists

Criteria difference calls for a new "red team" approach

The “Impediments” Team

Intentional Disruptions

- Predominantly intelligent actor attacks
- Tests run with three levels of information
  - No internal information
  - Internal configurations
  - Full internal knowledge
- Addresses system proactive and reactive responses

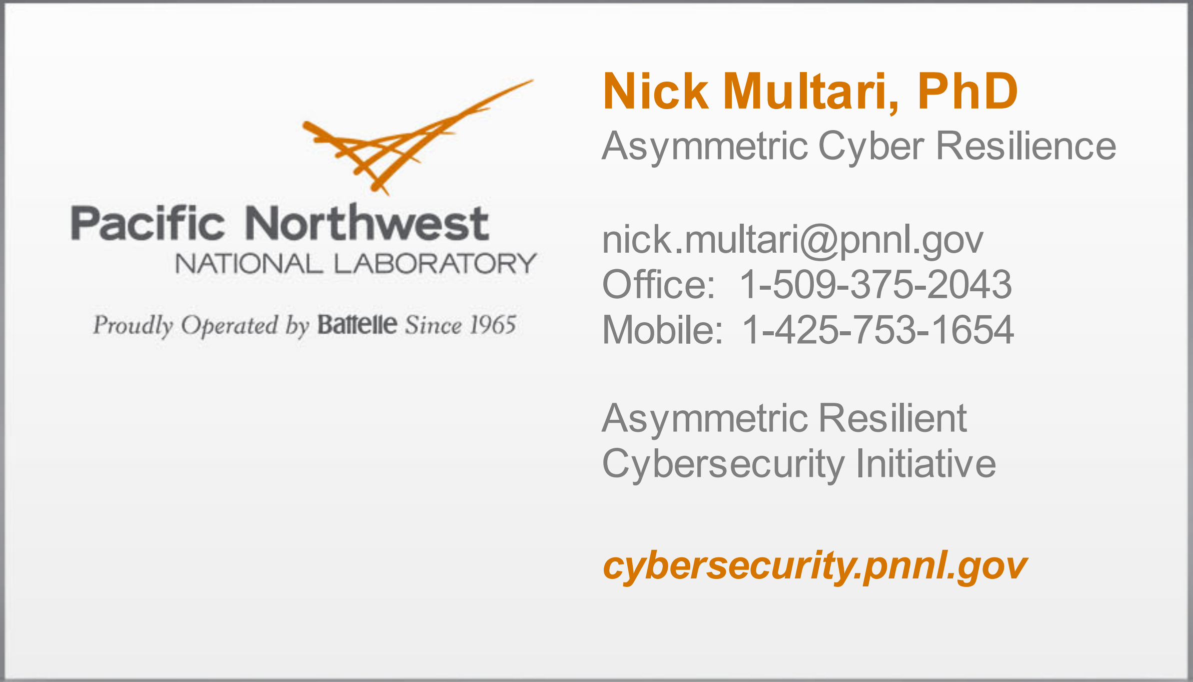
Natural Disruptions

- Includes environmental issues and equipment failures
- Scripted and injected at random points

- Must determine the critical threshold time limit for declaring success

Blue Sky Questions

- What does it even mean to have an asymmetric advantage in resilient cyber systems?
- By what measure(s) do we determine asymmetry?
  - Effectiveness?
  - Cost?
  - Risk?
  - …?
- What balance should we be trying to shift?
  - Adversary's cost/our cost?
  - Our cost/value of protection?
- Who pays for this?
  - Incentivize resilience that favors an asymmetric advantage for defenders? (how?)
  - Disincentivize non-use?
- How do we measure/prove the asymmetric advantage has shifted?
  - How complete does the test environment need to be?
  - What is the minimum configuration?
  - What metrics are needed?



Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Nick Multari, PhD
Asymmetric Cyber Resilience

nick.multari@pnnl.gov
Office: 1-509-375-2043
Mobile: 1-425-753-1654

Asymmetric Resilient
Cybersecurity Initiative

cybersecurity.pnnl.gov