

*Schematic of State-space Based Formulation Showing a Cyber System Operating Under Normal (Green), Marginal (Yellow), and Compromised (Red) States. Resilience is a measure of the degree to which the system can continue to meet mission when perturbed. Resilience requires system design to minimize the ability to transition into marginal and compromised states (robustness), and algorithms for rapid reconstitution when such transition occurs.*

## Theory of Resilience: A Framework for Resilient Design and Reconstitution of Cyber Systems

### Objective

Manipulation of data, computing, or coordination are the most impactful ways for preventing a system from realizing its mission goals. We are investigating a theoretical framework for resilience and effective autonomous reconstitution of compromised cyber systems with the goal of maintaining mission-critical operations in the face of disruptions.

### Approach

We hypothesize that resilience is achieved by a combination of specific cyber system design actions and control actions (usually after an event). The notion of controllability of cyber systems leads to a mathematically rigorous definition of resilience as the degree of stability of the system at or near any operational state, and defines the conditions on system dynamics, connectivity, and control input locations. Given this definition of resilience, the problems of robust system design and reconstitution may both be defined in terms of a multi-objective optimization problem, and resulting solutions provide insights into tradeoffs between resilience, cost, risk, and other relevant metrics.

### Achievements

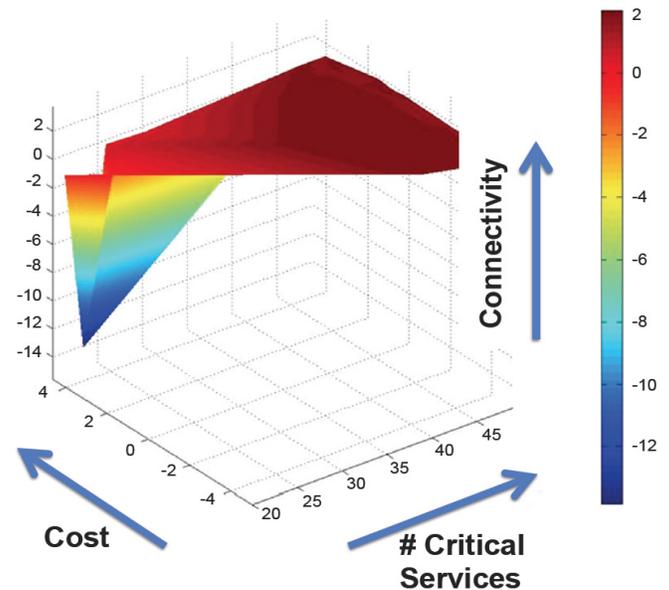
We developed a state-space based formulation that uses key properties of cyber systems. System dynamics, controllability, and stability analysis provide a quantitative approach to characterizing resilience. This formulation may be employed to design robust systems and dynamic autonomous reconstitution towards maintaining critical services in compromised cyber systems. Natural faults or attacks are modeled in this framework through their effect. The framework supports natural and adversarial faults by allowing independent and dependent fault sequences. A multi-objective optimization routine was applied to simplified cyber systems where faults were introduced at specified locations within the system. The objective was to determine a new configuration (connections, services, and their host computers) that enabled continuity of operations while improving resilience. The project has published three conference papers and submitted one journal paper based on this research.

## Impact

Natural and intentional manipulation of data, computing, or coordination are the most impactful ways that an attacker can prevent a system from realizing its mission goals. The results of this project will provide the technical basis for quantifying resilience in cyber systems and developing and evaluating approaches to robust design and autonomous reconstitution efforts in compromised cyber systems. This research will provide a mechanism for evaluating and prioritizing (for deployment) techniques for resilience based on relevant metrics.

## Future Work

- Perform analytical studies using simple topologies and linear dynamics
- Conduct simulation studies to understand stability of operational state to variations in state, graph, and input signals
- Integrate theoretical framework and response models into simulations
- Begin integration with other ARC projects for in-depth assessment of theory and identifying shortcomings
- Disseminate findings to other ARC projects and assist in integration as needed.



*Illustration of Multi-objective Optimization for Reconstitution on a Synthetic Random System*

## ABOUT

### The Asymmetric Resilient Cybersecurity Initiative

Researchers at PNNL are delivering the theory, processes, methodologies, and algorithms that will enable a resilient cyber infrastructure with an asymmetric advantage to thwart adversaries who seek to infiltrate and damage our national security through digital means. This exploratory science in Laboratory Directed Research and Development effort is made possible by the Pacific Northwest National Laboratory through funding provided by the U.S. Department of Energy.

For more information on the science you see here, please contact:

#### **Pradeep Ramuhalli**

Pacific Northwest National Laboratory  
P.O. Box 999, MSIN: K5-26  
Richland, WA 99352  
(509) 375-2763  
pradeep.ramuhalli@pnnl.gov