Mission Assurance: An Operational Imperative

AFCEA/GMU Critical Issues in C^{4}I Symposium

Harriet G. Goldman

May 23, 2012

MITRE

Approved for Public Release: 12-2460 – Distribution Unlimited

Why is Resiliency Important?

Skilled Adversaries

Traditional IA Practices

Computer Architectures

Fiscal Pressures

Critical Missions Fail When Attacked

What is Resiliency and How is it Achieved?

- The ability to provide and maintain an acceptable level of service in the face of faults and challenges to normal operation*

- ts:

in

-

be

limited, unknown, and possibly unknowable?

  - Includes deterrents to disrupt, confuse and impede adversary

Critical missions complete successfully despite effective cyber attacks against underlying technology

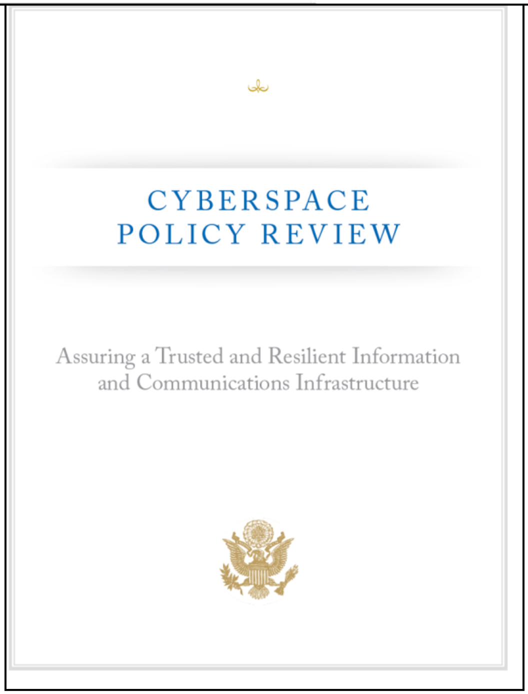
*Sterbenz & Hutchison, "ResiliNets: Multilevel Resilient and Survivable Networking Initiative", University of Kentucky & Lancaster University, http://www.ittc.ku.edu/resilinets/index.html

Government Recognition of Resilience

> *"Defending against these threats to our security, prosperity, and personal privacy requires networks that are secure, trustworthy, and resilient."*
>
> \- 2010 National Security Strategy

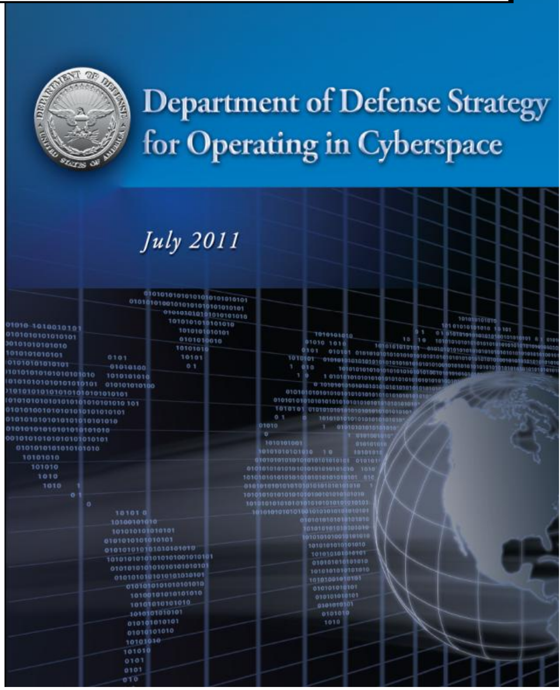
THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY VOLUME 9 NUMBER 8



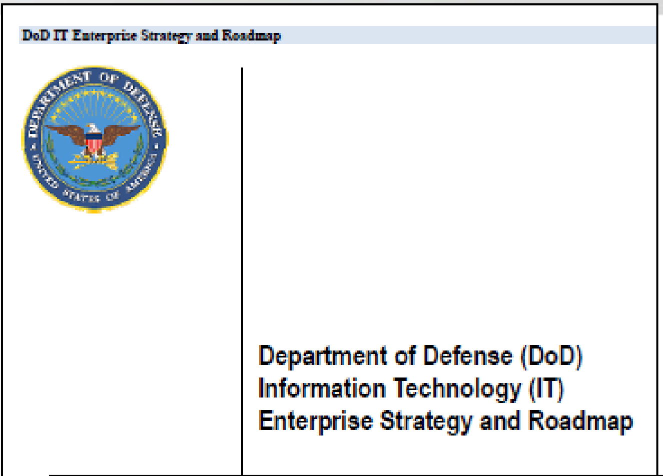
CYBERSPACE POLICY REVIEW

Assuring a Trusted and Resilient Information and Communications Infrastructure



Department of Defense Strategy for Operating in Cyberspace

July 2011



DoD IT Enterprise Strategy and Roadmap

Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap

Moving Toward Cyber Resilience

Bradford Willke, Cyber Security Advisor (Mid-Atlantic Region)

Cyber Security Evaluation Program

National Cyber Security Division

Central Ohio Infragard

Columbus, Ohio

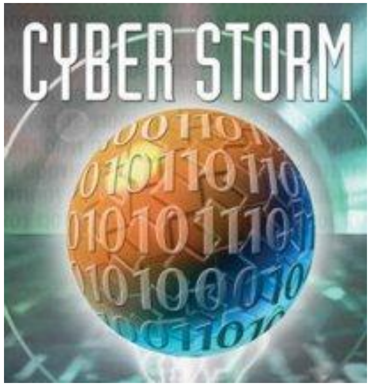
27 July 2011

Homeland Security

National Cyber Security Division

MITRE

Response



WELCOME

Secure and Resilient

Cyber Architectures Conference

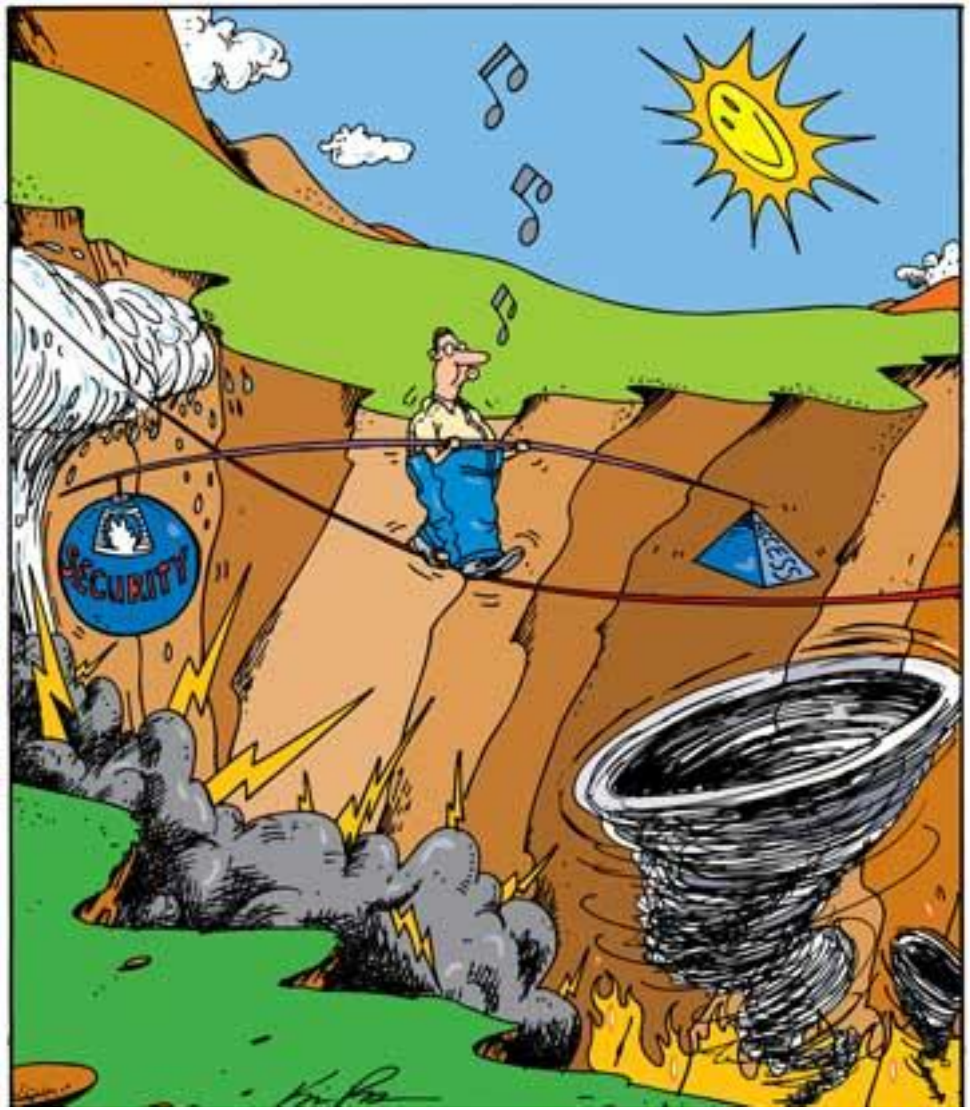
Resiliency | Agility | Assuring Effective Missions

Foundations of Trust

Homeland Security

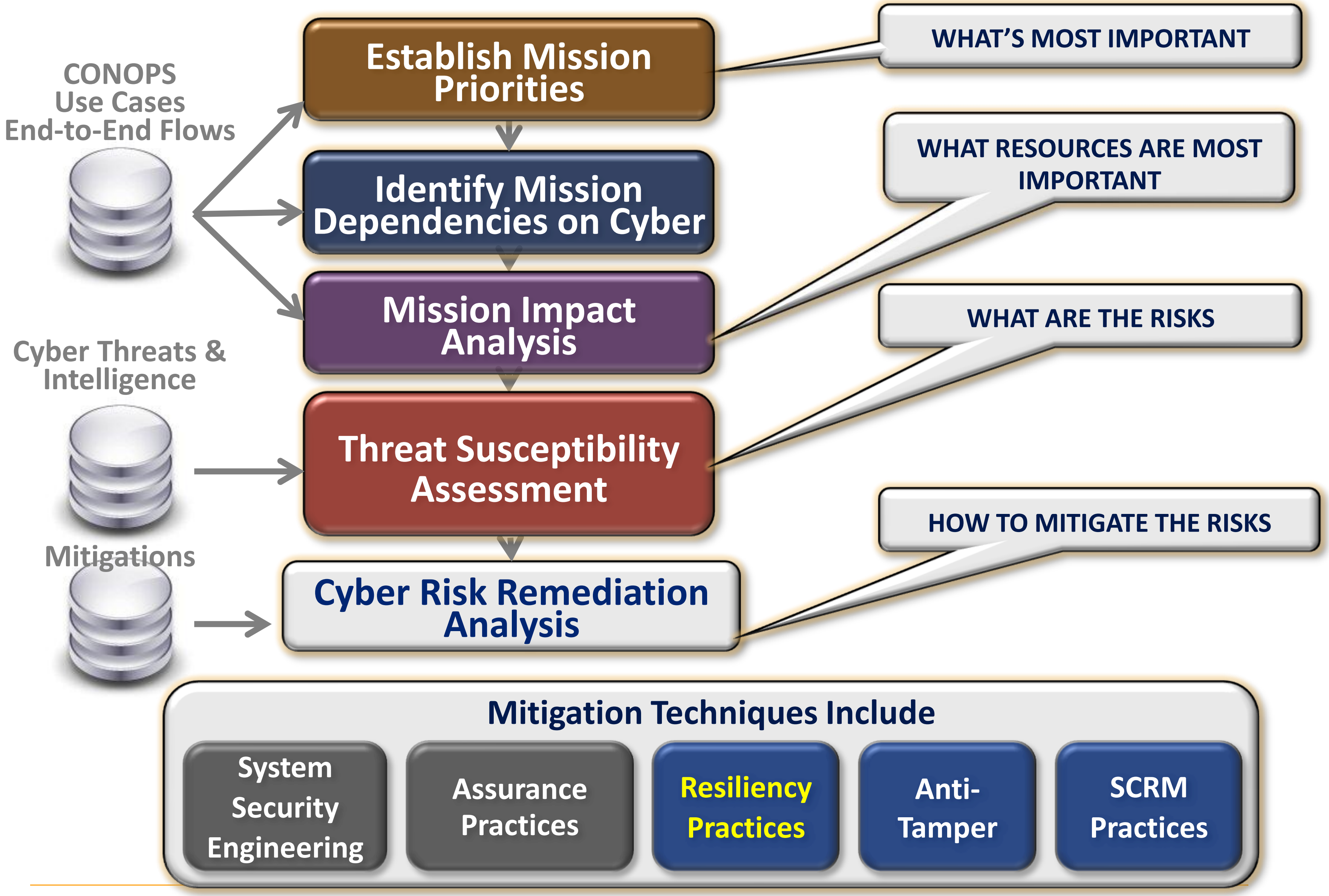
Science and Technology

Continuity of Critical Ops While Under Attack



- Failover, capacity, redundancy, COOP, and DR planning
- Configuration management
- Minimal essential priority
- Monitoring and correlation
- Consequence management
  - Gracefully degrade
  - COA Tactics, Techniques, and Procedures (TTP*s*)
  - Reconfigure
  - Isolate
- Recovery
  - Reconstitute minimal essential functions
  - Assess damage
  - Restore trust

Mission Assurance Engineering Framework



CONOPS
Use Cases
End-to-End Flows

Cyber Threats &
Intelligence

Mitigations

Establish Mission Priorities

Identify Mission Dependencies on Cyber

Mission Impact Analysis

Threat Susceptibility Assessment

Cyber Risk Remediation Analysis

WHAT'S MOST IMPORTANT

WHAT RESOURCES ARE MOST IMPORTANT

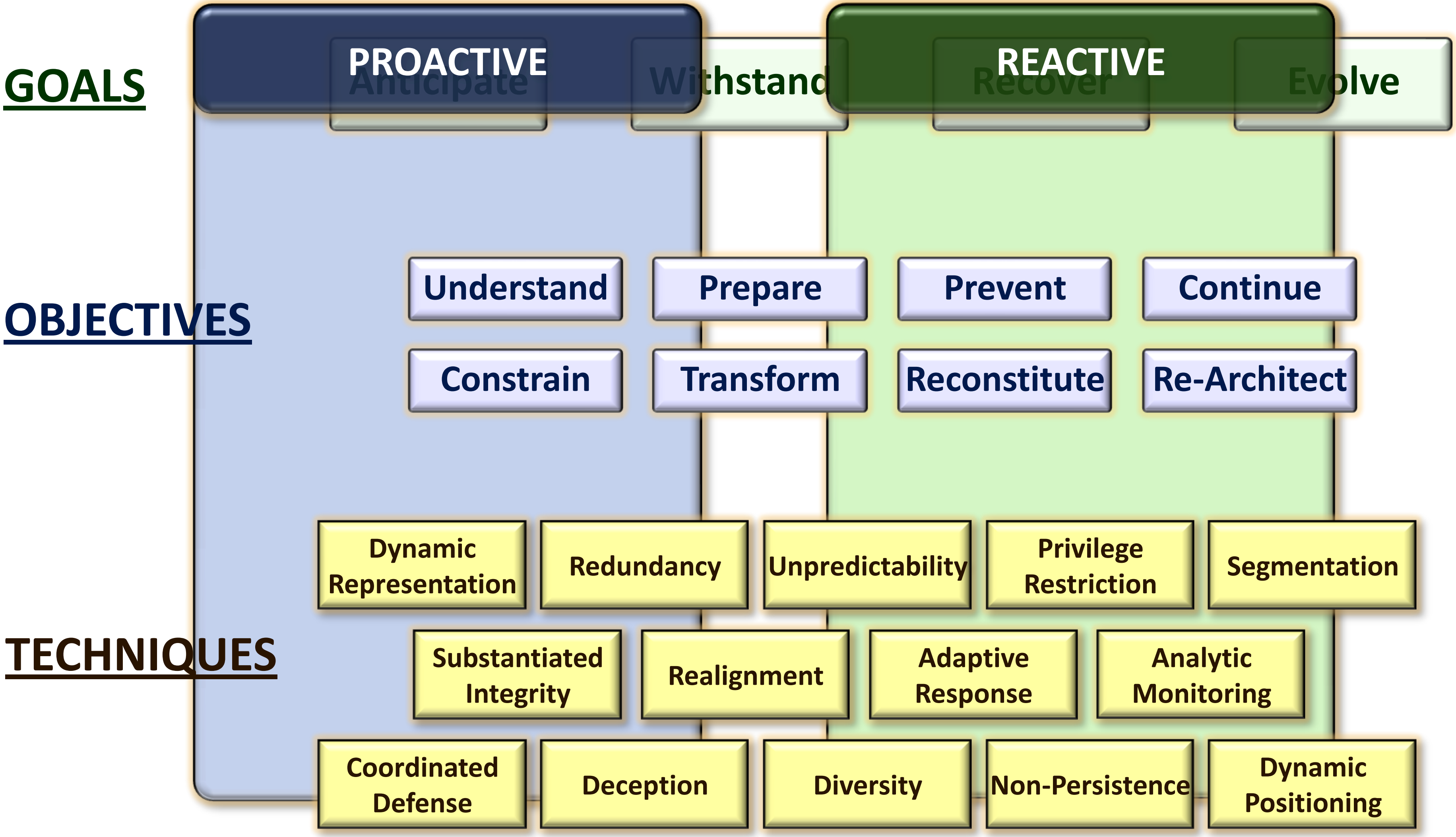
WHAT ARE THE RISKS

HOW TO MITIGATE THE RISKS

Mitigation Techniques Include

- System Security Engineering
- Assurance Practices
- Resiliency Practices
- Anti-Tamper
- SCRM Practices

Cyber Resiliency Foundation Elements



GOALS

PROACTIVE

REACTIVE

Anticipate

Withstand

Recover

Evolve

OBJECTIVES

Understand

Prepare

Prevent

Continue

Constrain

Transform

Reconstitute

Re-Architect

TECHNIQUES

Dynamic Representation

Redundancy

Unpredictability

Privilege Restriction

Segmentation

Substantiated Integrity

Realignment

Adaptive Response

Analytic Monitoring

Coordinated Defense

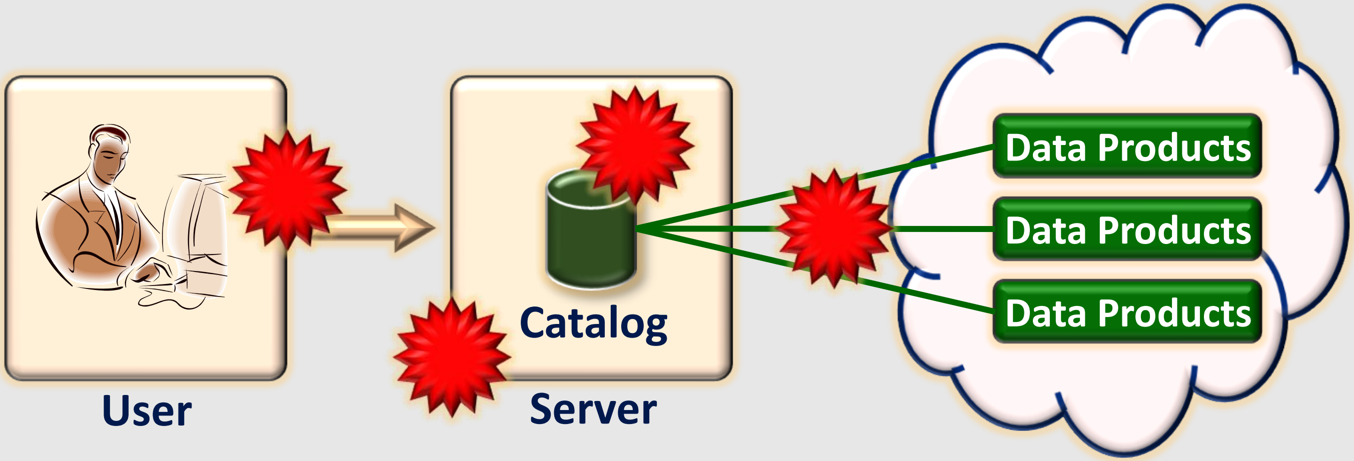
Deception

Diversity

Non-Persistence

Dynamic Positioning

Resiliency Framework



Goal	Objective	Technique	Technology	Metric
Withstand	Constrain	Deception	Deception Network	---
		Segmentation	Hardware trusted path	---
		Privilege Restriction	Fine-grained controls	---
Recover	Reconstitute	Redundancy	RIAK	---
			multi-cloud storage	---
	Continue	Substantiated Integrity	Crypto bindings	---

MITRE

Summary

- Achieving cyber mission assurance requires we
  - Change how we think about cyber threats, security approaches, and trust
  - Adopt new risk management and system engineering processes
  - Design, build, and integrate mission critical systems for resilience
  - Develop agile operations and decision support capabilities
  - Measure meaningful metrics
  - Define policies and practices to promote resilience
  - Collaborate and partner to change the game

Sun Tzu

“If your enemy is secure at all points, be prepared for him.

If he is in superior strength, evade him.

If your opponent is temperamental, seek to irritate him.

Pretend to be weak, that he may grow arrogant.

If he is taking his ease, give him no rest.

If his forces are united, separate them … appear where you are not expected.”

Thank You !

Questions?

Harriet Goldman

hgoldman@mitre.org

MITRE