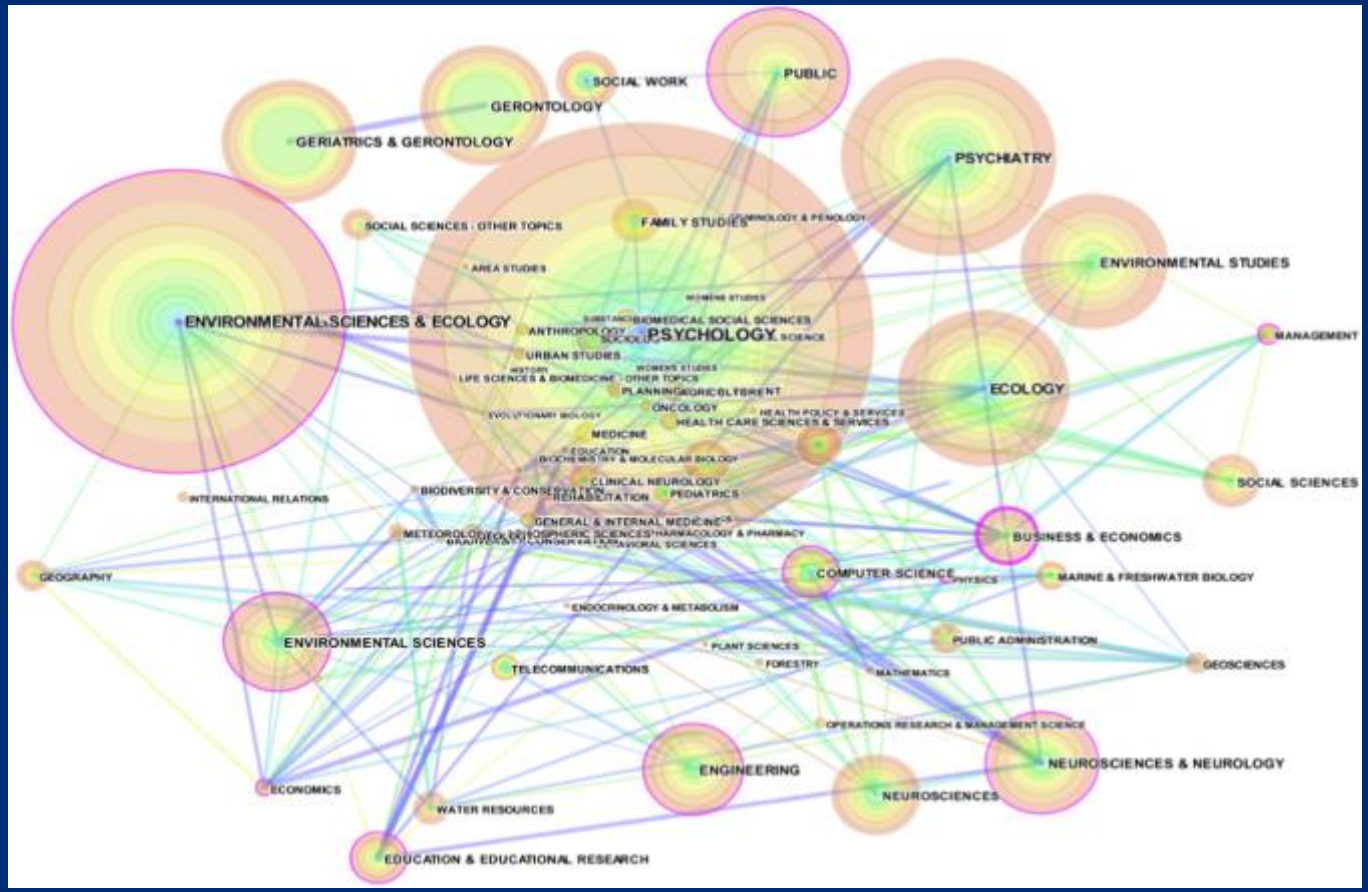
A Program Framework for Cyber Resilience

Rose Daley
(Rose.Daley@jhuapl.edu)
Scott Casper
(Scott.Casper@jhuapl.edu)

Resilience is NOT New



Features ….

Good Engineering

- **Anticipate**
- **Withstand**
- **Recover**
- **Evolve**

Hosseini, S., Barker, K., & Ramirez-Marquez, J. E. (2016). A review of definitions and measures of system resilience. Reliability Engineering & System Safety, 145, 47–61cc

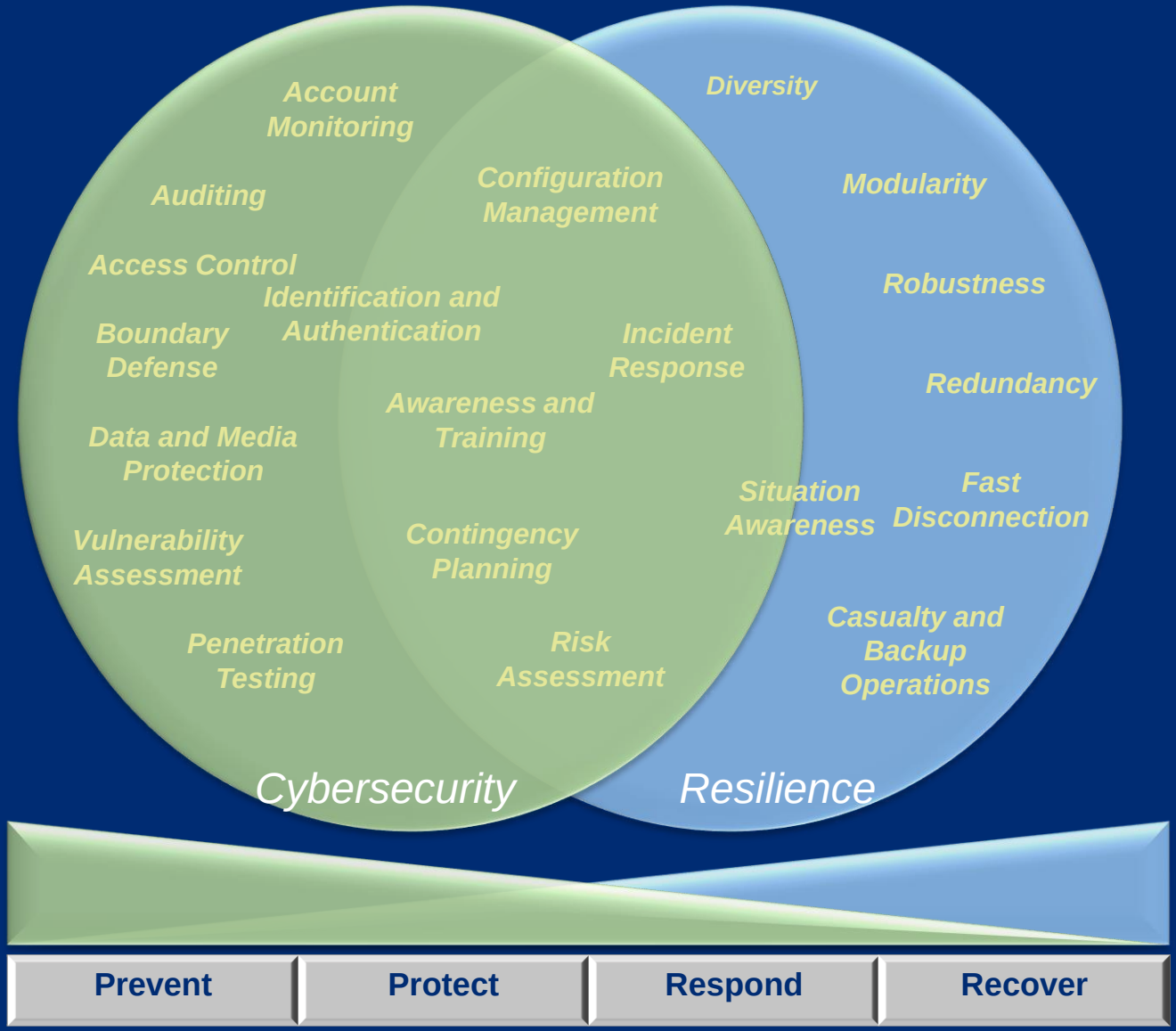
Resilience Papers by Domain, 2000-2015, CiteSpace

System Resilience and Cyber Resilience

Traditional System Resilience	***Cyber Resilience***
Resilience to unexpected events • Faults/failures and battle damage • Data corruption (integrity) and system availability • Safety • Graceful degradation outside designed performance envelope	Resilience to intentional, covert, remote actions • Faults/failures, damage, data corruption created by adversary
	Existing resilience features not always effective in cyberspace • Physical redundancy is not cyber redundancy
Kinetic weapons arsenals and physical faults/failures relatively well-understood	Cyber weapons evolve rapidly • Hard to predict adversary capability • Hard to predict all of the effects
Confidentiality, if considered at all, handled separately	Confidentiality always considered

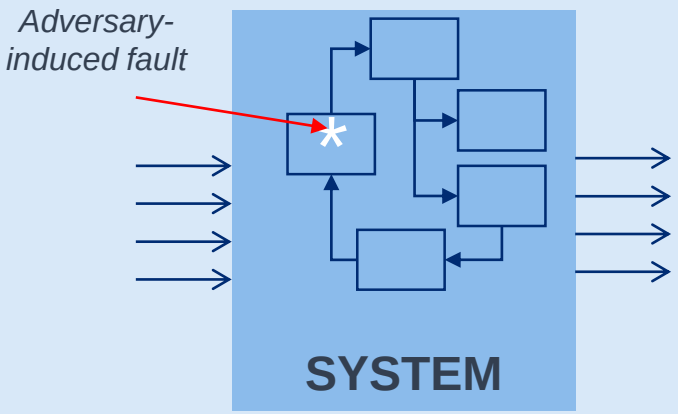
Cybersecurity and Resilience

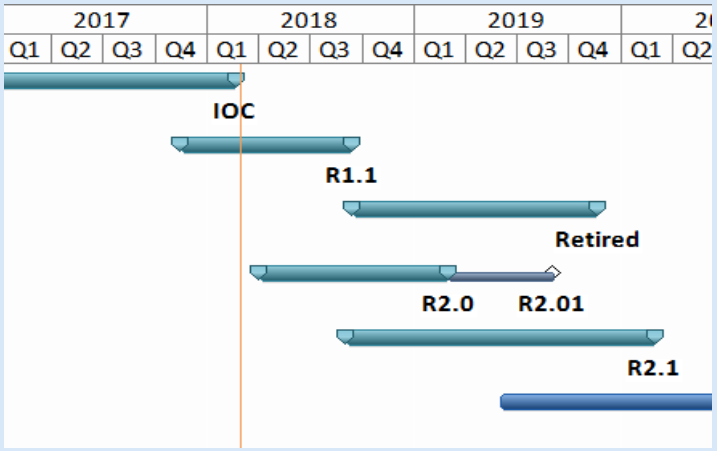
- Similar concerns, different emphasis
- Potential to interfere with or inhibit each other
- Awareness, evaluation, and careful trade-off



Cyber Resilience Extends Beyond the System

- **System Resilience**
  - Persistence of ***designed functions and performance***
  - In the face of disturbances both known and unknown (mission survivability)
- **Program Resilience**
  - Persistence of ***capabilities throughout the complete program lifecycle***
  - In the face of uncertainty at the program level (threats and failures to system and support structure)





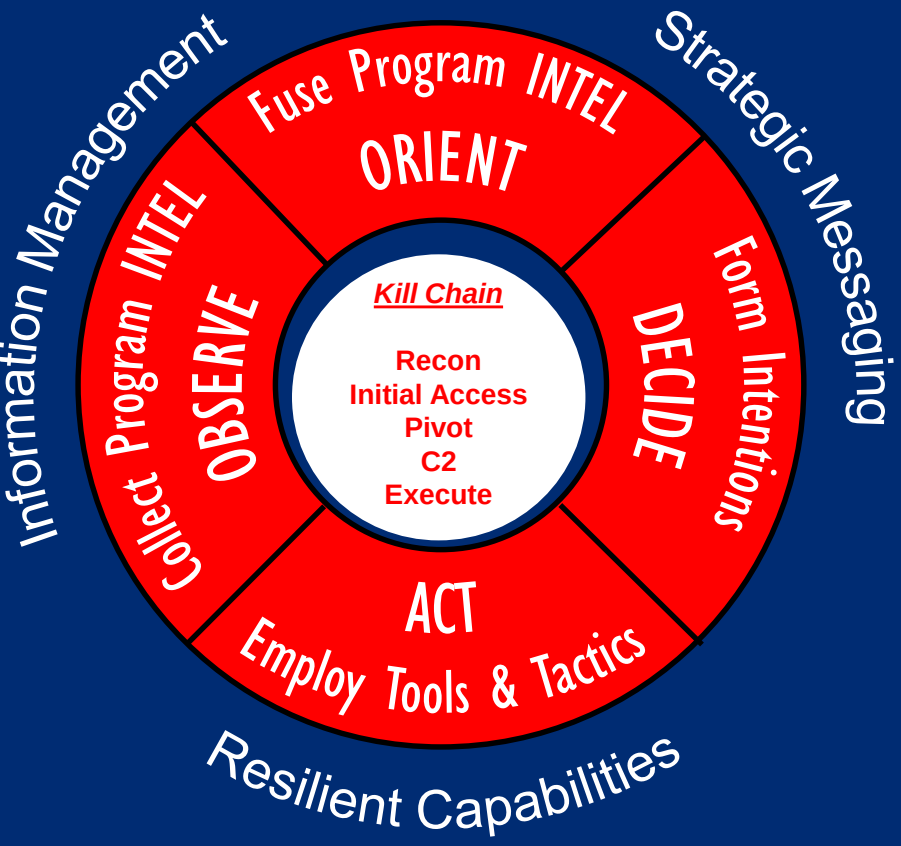
Cyber Decision Cycle Defeat Concept

Strategic Messaging
Disrupt Adversary Decision-making

Resilient Capabilities
Agility to Adversary Measures and Counter Measures

Information Management
Actively Control Information and Disrupt Adversary Collection

Effective Use of the Risk Management Framework and System Engineering



Continuous, Integrated Disruption of the Adversary's Decision Process Throughout Our System's and Program's Lifecycle

What is a Resilient Program?

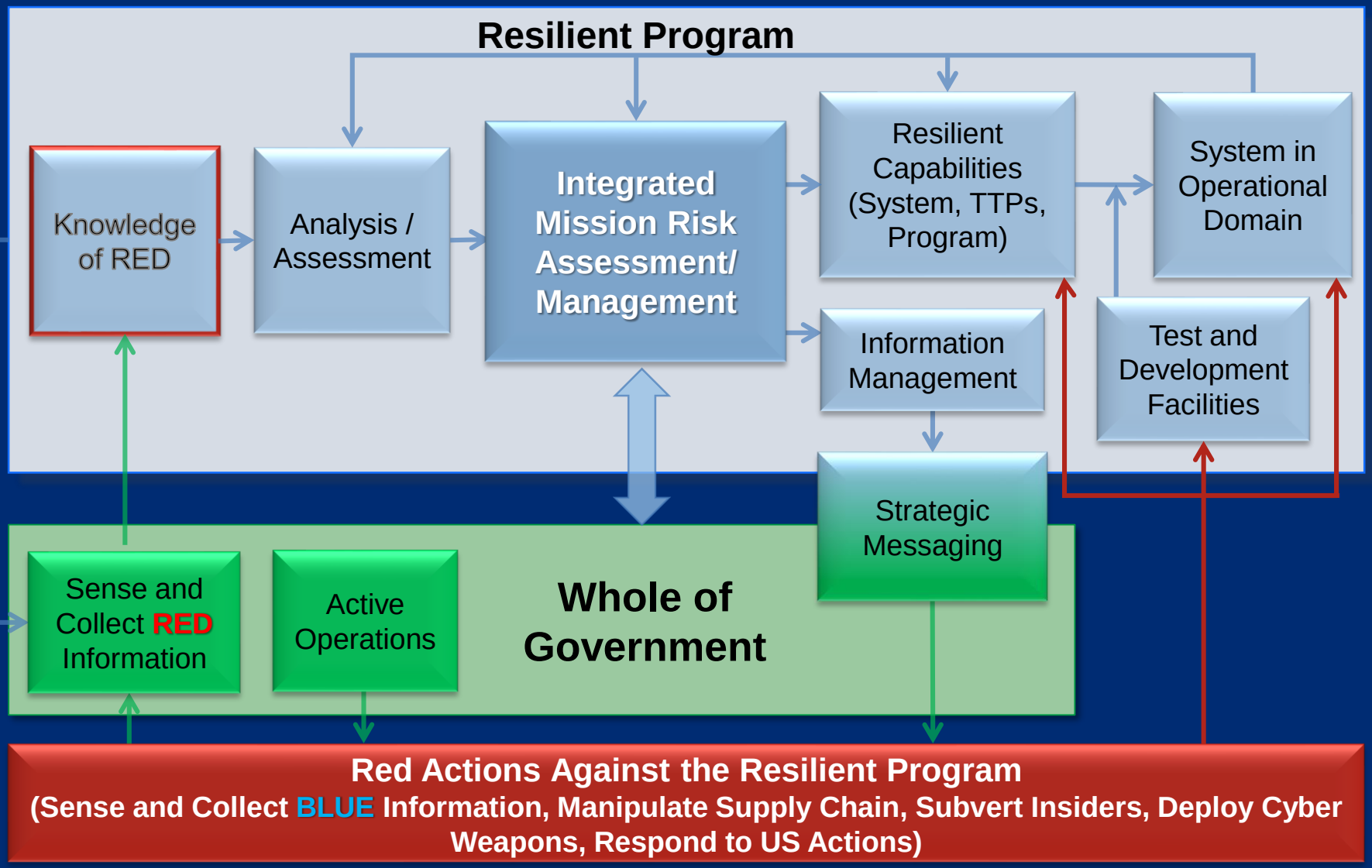
A Resilient Program Provides Overarching Support and Coordination

A Program of Record (POR) with:

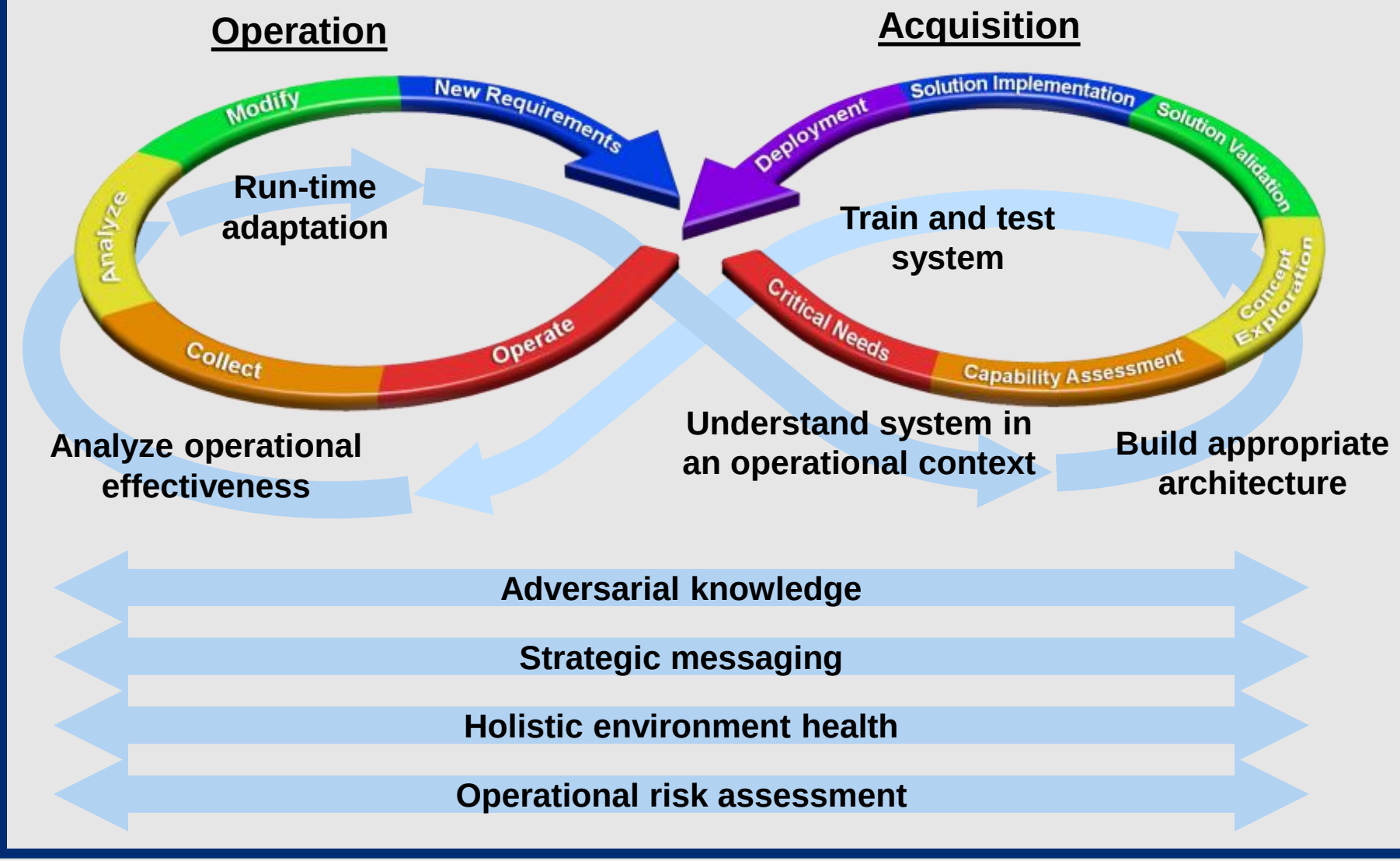
- ***resilient capabilities*** exhibiting robust, agile, and responsive elements
- actively addressing rapidly evolving adversary kill chains
- proactively managing all-source risk
- and intentionally influencing all internal and external program information flow.

- **Know System and Program Details**
  - *Identify and Define System Interdependencies*
  - *Comprehensively Understand Program Information and Implications*
- **Shape Information for Defender's Advantage**
  - *Information Management (Control Our Information)*
  - *Strategic Messaging (Influence Adversary Understanding)*
- **Define Solutions for Rapid Evolution and Improvement**
  - *Resilient System Capabilities*
  - *Aggressive Testing*

(U) Resilient Program Framework



Framework Applies Throughout the Life Cycle



Resilient Capabilities

How will you continue to operate when you're compromised?

Feature	Description	Implications for Cyber Resilience
Diversity	Differently designed or implemented modules with (nearly) the same functionality.*	Multiple techniques required to degrade a particular function; can reduce scope of an intended attack.
Modularity	Functions are cleanly encapsulated and dependencies between functional modules are minimized.	Helps contain system failures and negative effects to a single or just a few modules.*
Robustness	System is effective in all or most situations and conditions.	Better able to recover from cyber attacks designed to cause failures; can also be robust against cyberspace-specific conditions like malware propagation and system re-infection.*
Redundancy	Duplicate components provide replacement capability when a primary component fails.*	Minimal if the redundant components are identical; if source of compromise can be removed prior to switchover, can provide rapid reconstitution and recovery.
Fast Disconnection	Ability to rapidly isolate subsystems, modules, or components while they continue to operate. Ideally, to also easily reconnect when the danger has passed.	Ability to continue operating in compromised environments, can also reduce the spread of malware and assist in diagnosing sources of infection.
Situation Awareness	Insight into the current state of the system to operators and to the system itself; includes an awareness of current threats and risks to the system.	Increases the ability to maintain and reconstitute system functions when compromised.
Casualty and Backup Operations	Ensure essential functions are still performed when the system fails or is compromised.	Appearance of a failure may prompt system-degrading actions; operator-performed casualty or backup operations may be isolated from cyber compromise.

*K.J. Hole, Anti-fragile ICT Systems, Springer, 2016, [online] Available: http://link.springer.com/book/10.1007/978-3-319-30070-2.

Evaluation Considerations for System Components

- Exposure
  - Externally accessible
  - Susceptibilities/known weaknesses
  - Known/preferred attack vector
- Defensive Position
  - Good visibility/reach into system
  - Good location for countermeasures
  - Access to mission critical functions and information
  - Access to diagnostics, logs and/or sensors
  - Ability to protect mission critical functions and information
- Recovery Enabler
  - Existing response/recovery capability
  - Access to protected storage and/or network

System Considerations (role of the component)

- Major System Upgrade
  - Leverage/expand planned development & test activities
  - Minimize program perturbation
- Technology Refresh
  - Replace with less susceptible parts
  - Replace with improved response/recovery
  - Replace with safer supply chain and/or anti-tamper countermeasures
- Program Risk
  - Threat environment
  - Risk of *not* improving
  - Program protection
- Program Dependencies
  - Time until next opportunity
  - Phased deployment

Program Considerations (opportunity and risk)

Information Management

What are you giving away?

- Test plans, procedures and results
- Design details
- Failure modes and impact
- Planned test dates and facilities
- Press releases

Strategic Messaging

What do you want them to think about your program?

- Program's public profile
  - Capabilities (current and planned)
  - Key contributors and suppliers
  - Key facilities

- Adversary's knowledge of program
  - Details of implementation and status
  - Sources of information
  - Ability to monitor

- Influence and management
  - Control of information
  - Details of successes and failures
  - Disinformation?

Implications for T&E

- Know your adversary
  - Exploits and vulnerabilities in systems under test
  - Exploits and vulnerabilities in test equipment
  - Threat intelligence
- Know your risk
  - 21st century→ “x shall do y” includes implied “even when compromised”
    - TEST THAT!
  - Manipulation of test results
  - Availability of facilities
- Control your information
  - Test plans, procedures, and results
  - Unmanaged telecons/product reviews
  - Press releases and public briefings

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY