Cybersecurity Developmental Test and Evaluation (DT&E) Lessons Learned

ITEA Cybersecurity Workshop

27-30 March 2017

Paul Dailey

JHU/APL

Paul.Dailey@jhuapl.edu

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

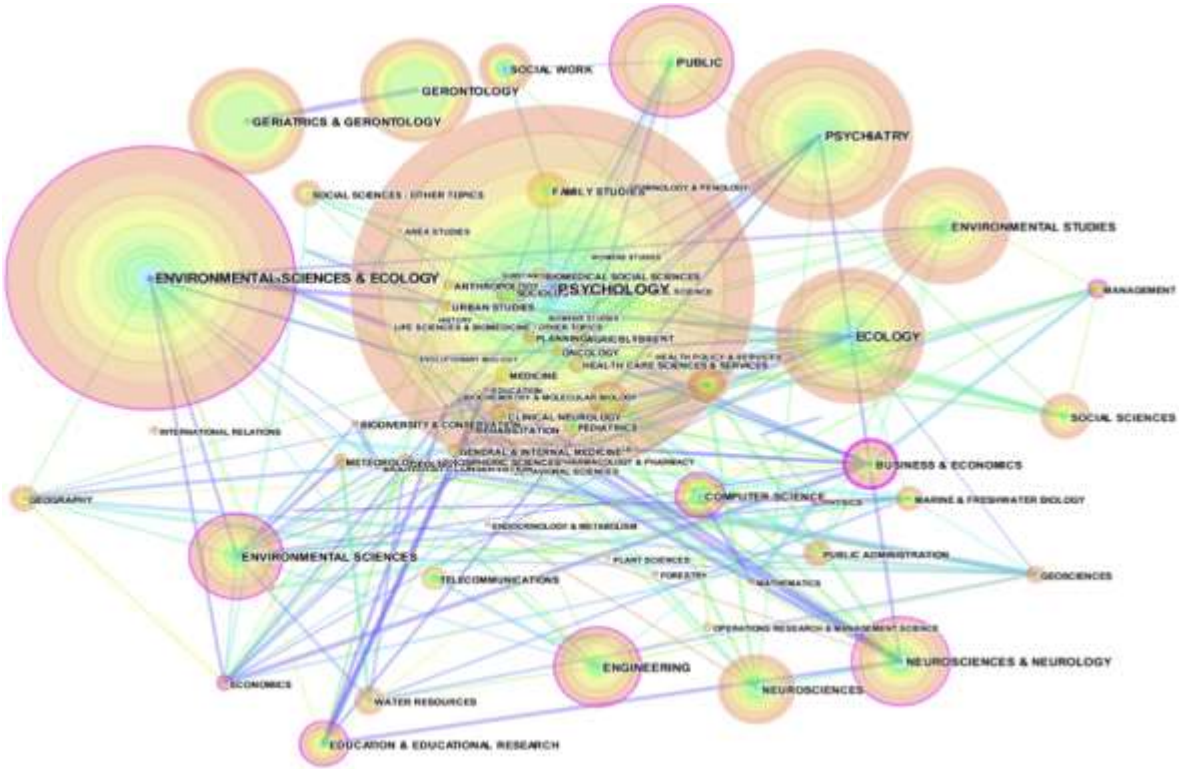
Agenda

- Purpose
- Context: Program and system resiliency
- Cyber T&E Activities: Evaluating a system's resilient capabilities
- Cyber DT&E lessons learned and recommendations

Briefing Purpose

- **To discuss the various cyber T&E activities, how they relate, and present some lessons learned from recent experiences**

Resiliency is NOT New



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

Features ….

Good Engineering

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

Through:

- **Diversity**
- **Modularity**
- **Robustness**
- **Redundancy**
- **Fast Disconnection**
- **Situation Awareness**
- **Casualty/Backups**

What is a Resilient Program?

A Resilient Program Provides Overarching Support and Coordination

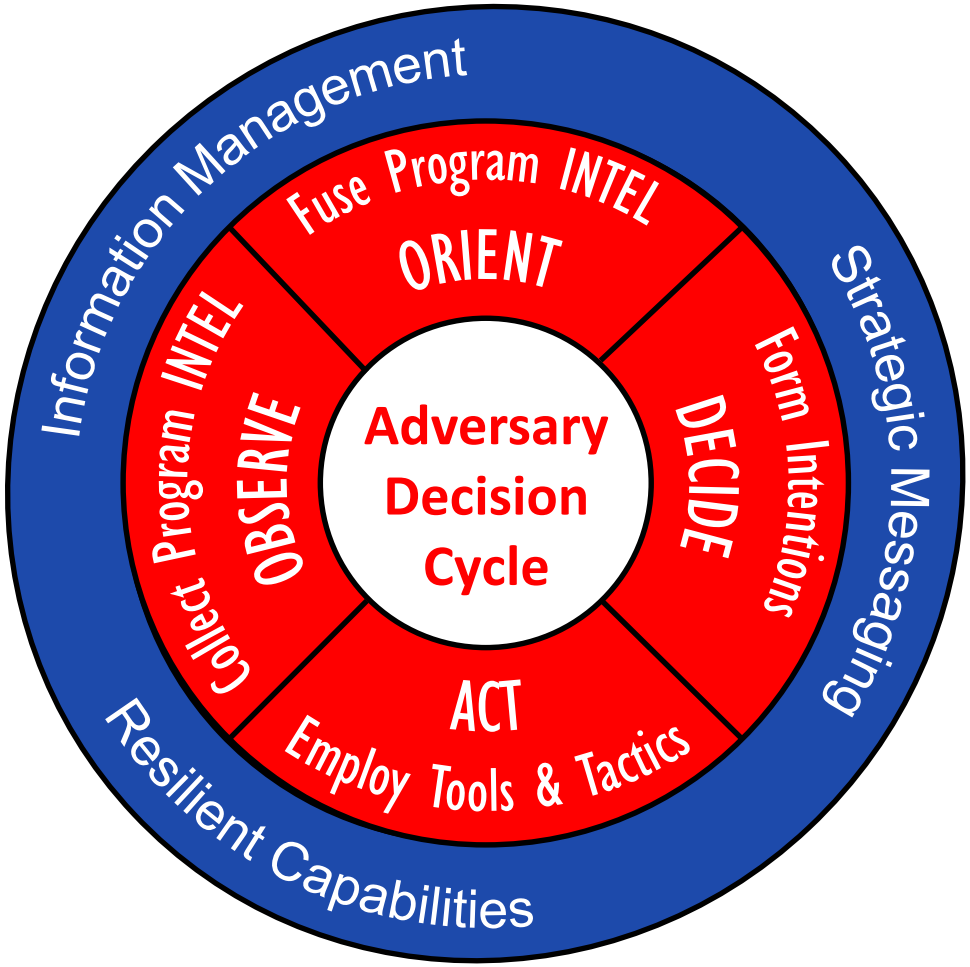
A Program of Record (POR) with:

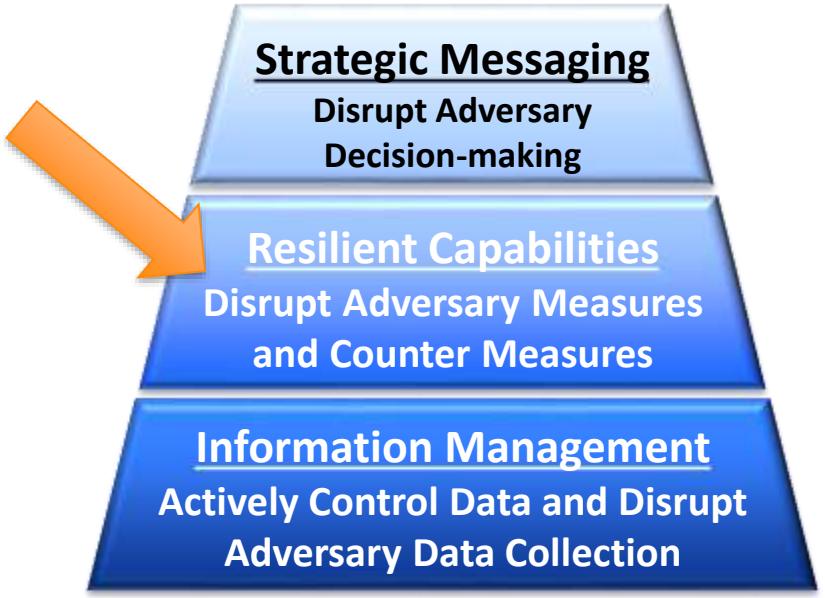
- ***resilient capabilities*** **exhibiting robust, agile, and responsive elements**
- **actively addressing rapidly evolving adversary kill chains**
- **proactively managing all-source risk**
- **and intentionally influencing all internal and external program information flow.**

- ***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***

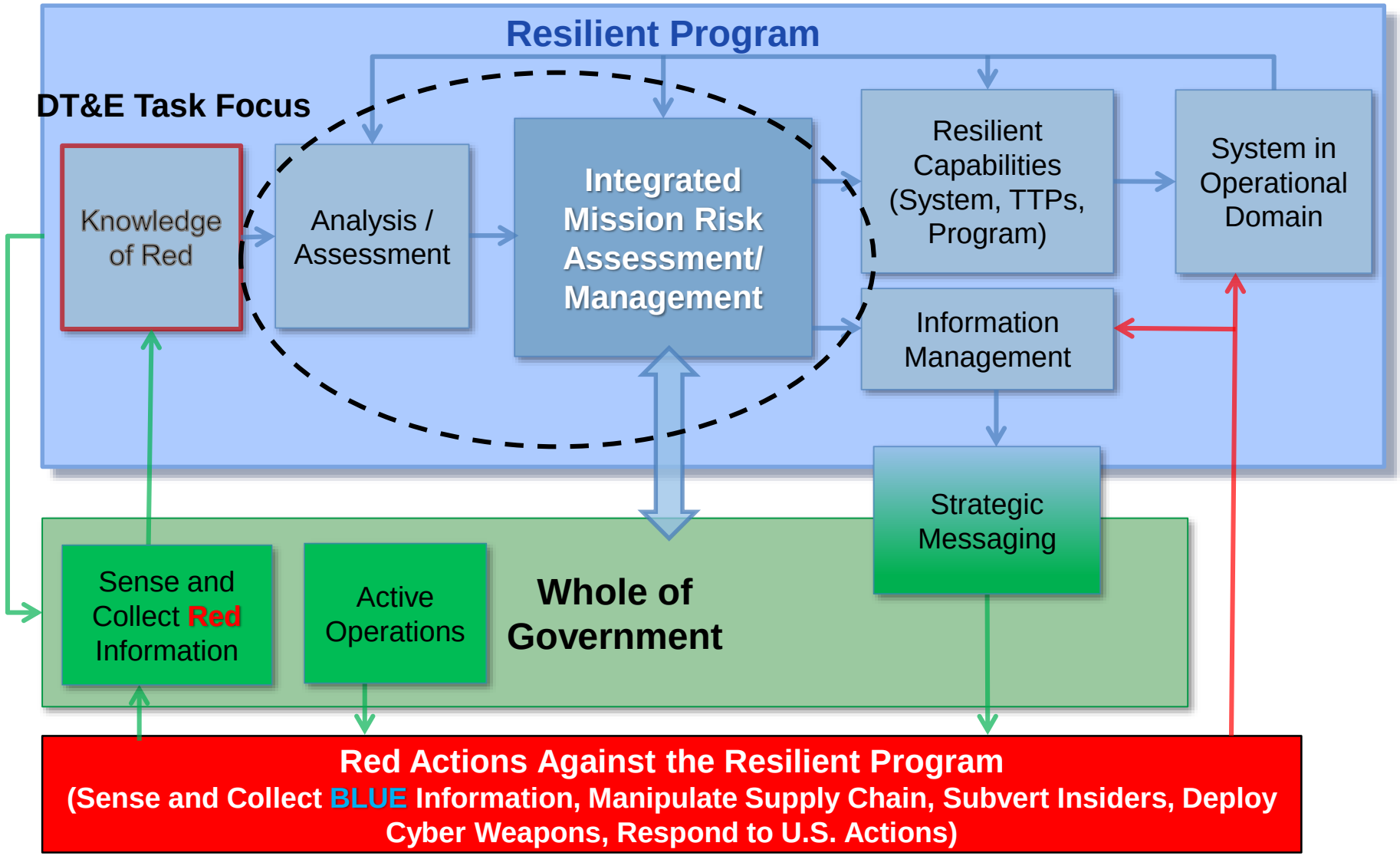
Cyber Decision Cycle Defeat (CD2)

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

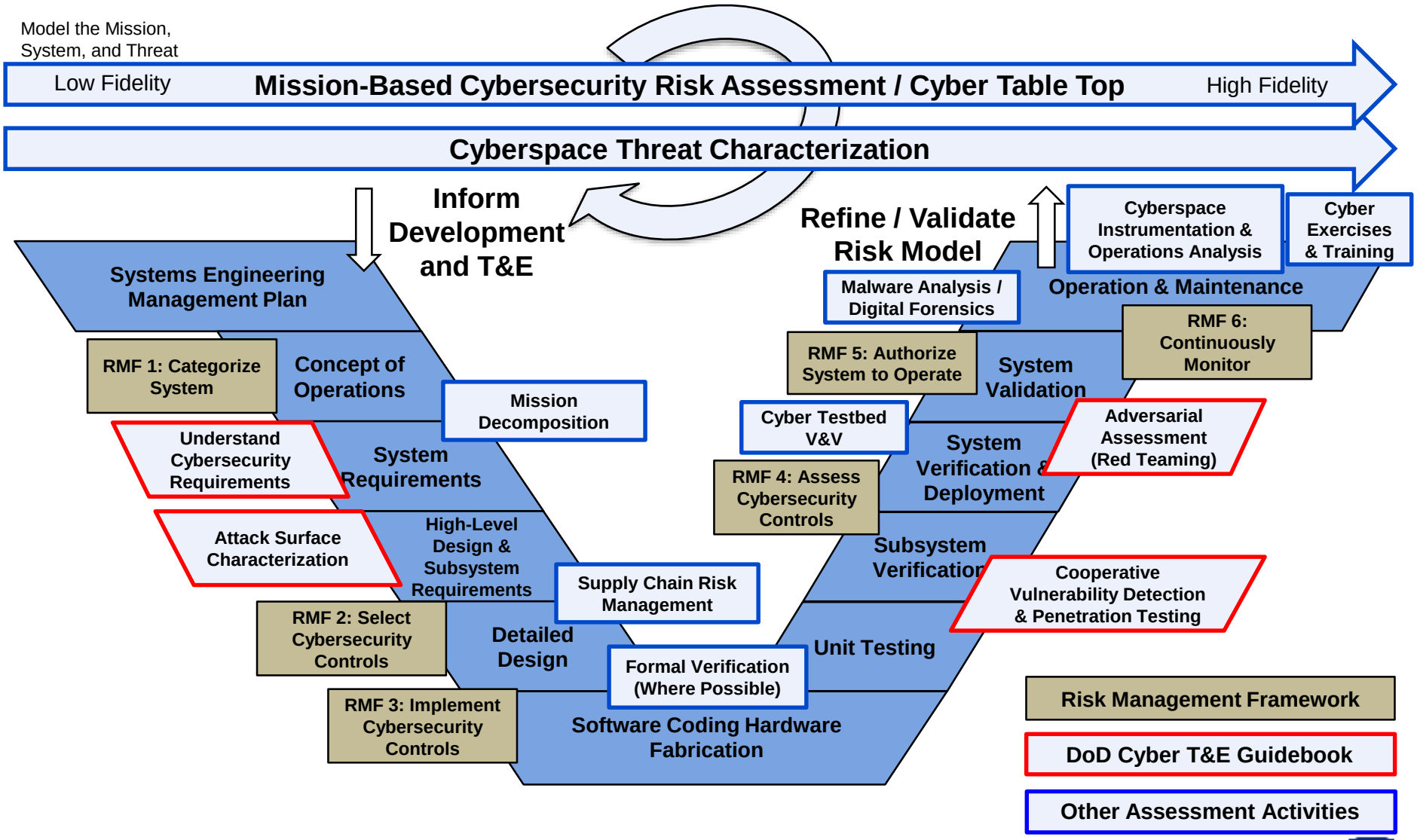




Resilient Program Concept



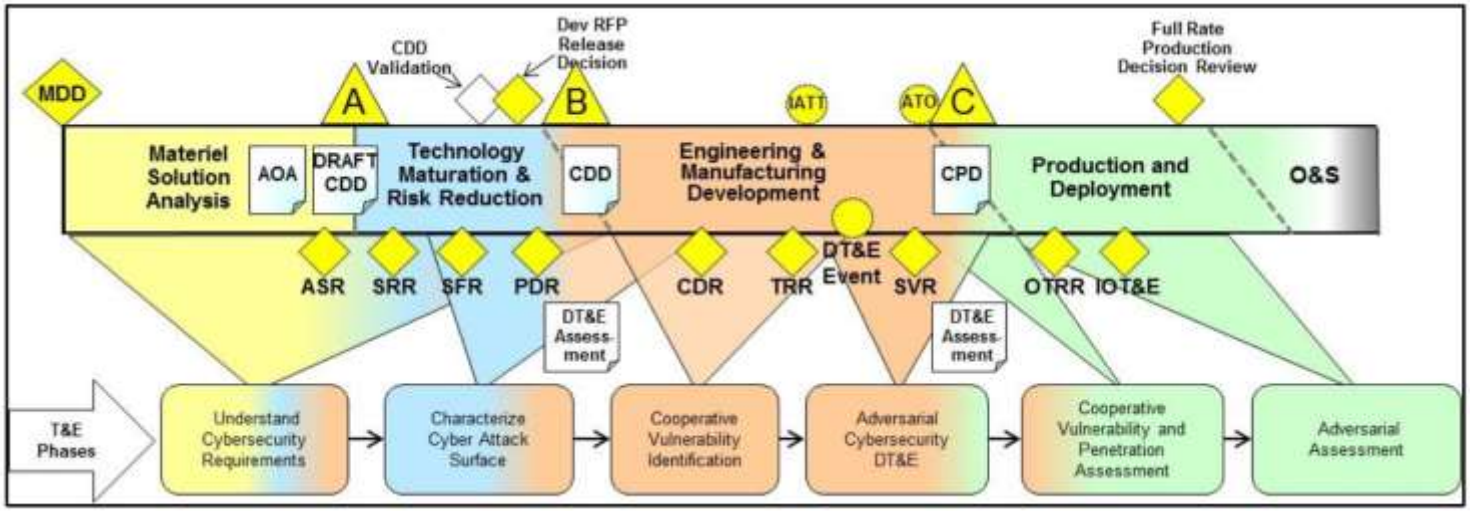
System Cybersecurity Assessment & T&E Activities



Some Cyber DT&E Recommendations and Lessons Learned

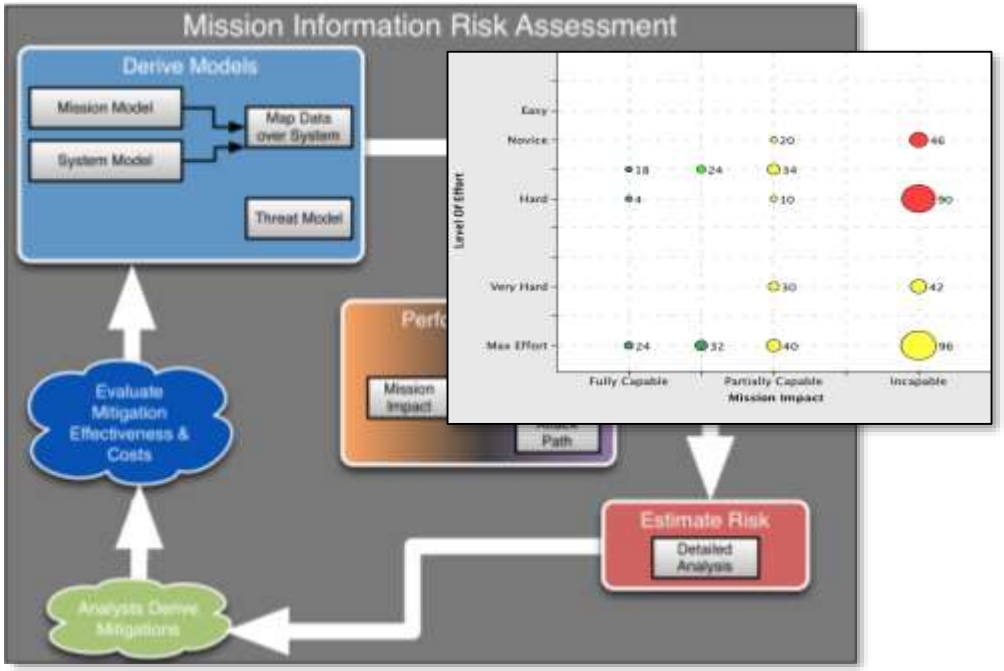
General Cyber DT&E Recommendations

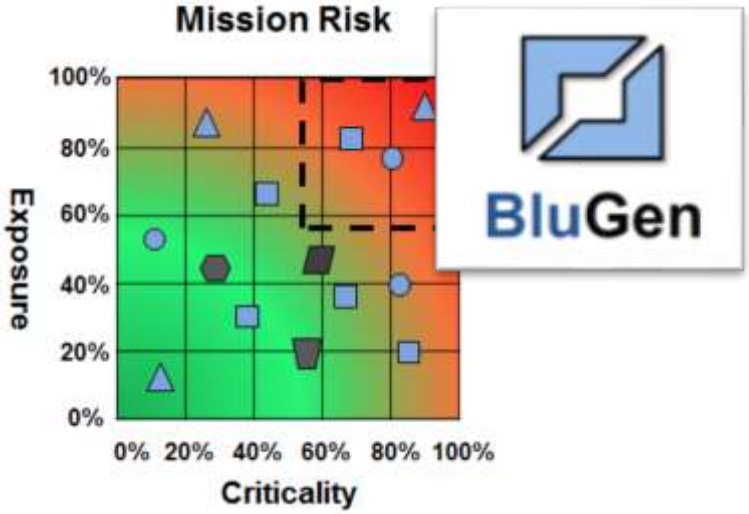
- **Start as early as possible (or better late than never)!**
  - **Mission decomposition / dependency analysis**
  - **Cyber risk assessments (CRA) and cyber table top (CTT) activities**
  - **Threat characterization / Intelligence Community (IC) engagement**
- **DT&E should evaluate the system design and use results to inform hands-on system assessments (implementation)**
- **Avoid duplication – Integrate cybersecurity into your systems engineering architecture products and models**



Start with a Cyber Risk Assessment or Table Top!

- **Many system vulnerabilities can be discovered through analysis of the mission, system, threat, threat and operating environment**
- **CRAs and CTTs can occur in any acquisition lifecycle phase**
  - **Brings together system designers, operators, security and red team**
  - **Consistent mechanism for communicating cybersecurity posture**





CRA/CTT Execution and Method Selection

- **Conduct an initial CRA/CTT on the system design. Use it to drive T&E. Update it based on DT&E results, or when the system, mission, or threat changes**

- **Multiple CRA methods are available – depending on the level of system maturity and available resources**
  - **DoD cyber table top exercises**
  - **Red-team driven system assessment (a different table top method)**
  - **Comprehensive model-based risk analysis**
  - **Qualitative (current) and quantitative (in research) methods**

- **Cyber risk assessments inform and can be updated by the following activities:**
  - **Requirements definition and validation**
  - **Attack surface characterization**
  - **Cooperative vulnerability and adversarial assessments**
  - **Malware analysis, operational monitoring, and cyber exercises**
  - **Supply chain and insider threat analyses**

CRA/CTT Participants and Vulnerability Management

- **Make designers, defenders, and operators part of the "red team"**
  - They know the system best
  - They can reduce the time required to confirm a vulnerability
  - "One team concept" reduces defensiveness
  - Drives developers to think differently

- **Prioritize vulnerabilities, and categorize them as:**
  - Confirmed – No reason to test further – Explore mitigation options
  - Plausible – These (prioritized) should drive cyber DT&E
  - Not a vulnerability in the actual system; occurs when design is different than implementation

- **Prioritize vulnerabilities based on**
  - Mission impact
  - Assessment of adversary capabilities and intent
  - Technical feasibility of exploit

CRA/CTT Mitigation Analysis and Management

- **Identify potential mitigations as vulnerabilities are discovered and hold a mitigation table top following CRA/CTT**

- **Prioritize mitigations based on:**
  - **Number of associated vulnerabilities mitigated and their ranking**
  - **Required resources, level of effort to implement (estimate)**
  - **Threat intelligence assessments**
  - **Location on the adversary's kill chain (farther upstream, the better)**

- **Close the loop with system cybersecurity requirements**
  - **Are the current requirements still valid?**
  - **What gaps exist, and what is the residual risk if not closed?**
  - **Are new requirements needed?**
  - **What test infrastructure requirements are needed for DT&E?**

Build Strong Relationships

- **Establish a cyber working group (CWG) and a cyber T&E working group that is part of the T&E Working Integrated Product Team (WIPT)**

- **Ties between systems engineering and cybersecurity help with:**
  - **Functional assessment: Defense Evaluation Framework (DEF)**
  - **Mission-based assessments: CRAs / CTTs and some T&E events**
  - **Goal is to integrate functional and mission analysis**

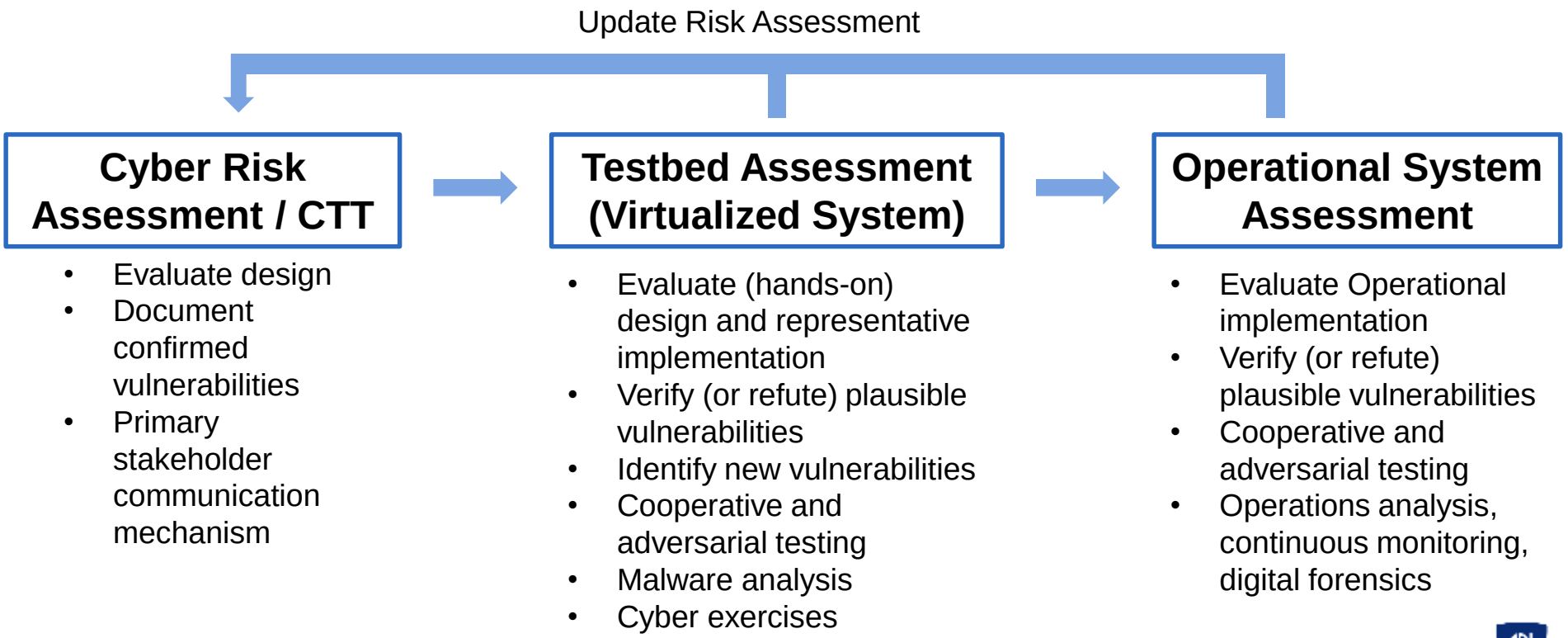
- **Build strong threat intelligence relationships**
  - **It is not only beneficial for red teams!**
  - **Programs should build strong relationships with the intelligence community and/or industry partners to share information**
  - **Knowledge of RED helps identify and validate assumptions used in CRA/CTT, cyber DT&E and related activities**

Recommendations for Systems Engineering

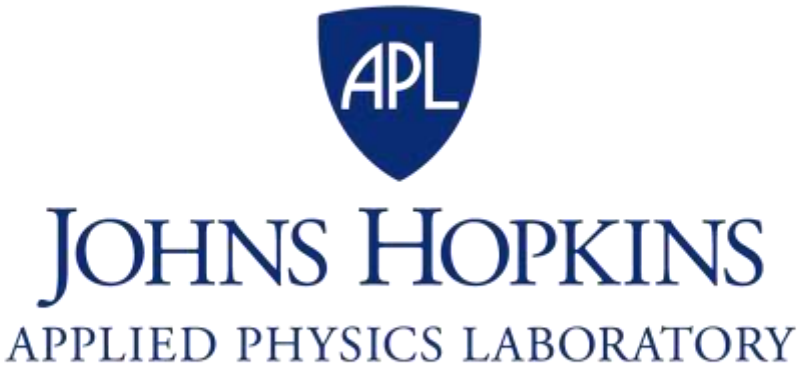
- **Integrate cybersecurity into the systems engineering process**
  - **Include cybersecurity requirements with system requirements**
  - **Represent cybersecurity in your systems architecture**
  - **Don't make cybersecurity a bolt-on activity**
- **Start identifying your cyber test infrastructure early**
  - **Utilize virtualization for system development and testing**
  - **Understand limitations of your virtualized solutions**
- **Design in and test cyber casualty modes**
- **Use activity and sequence diagrams to define what normal system comms / behavior looks like, collect data and compare!**
- **Make RMF work for you**
  - **Trace design-related controls to cybersecurity requirements**
  - **Align process-related controls to cyber assessment & T&E activities**
  - **Don't treat it as a separate activity**

Recommendations for Cyber T&E Practitioners

- **Define a T&E process that works for fielded systems, not just new acquisition programs**
- **Bring in OT&E early, allow them to witness, integrate, and reuse testing where possible**
- **Iterate cybersecurity DT&E with <u>each</u> development cycle**



Questions?


APL
JOHNS HOPKINS
APPLIED PHYSICS LABORATORY