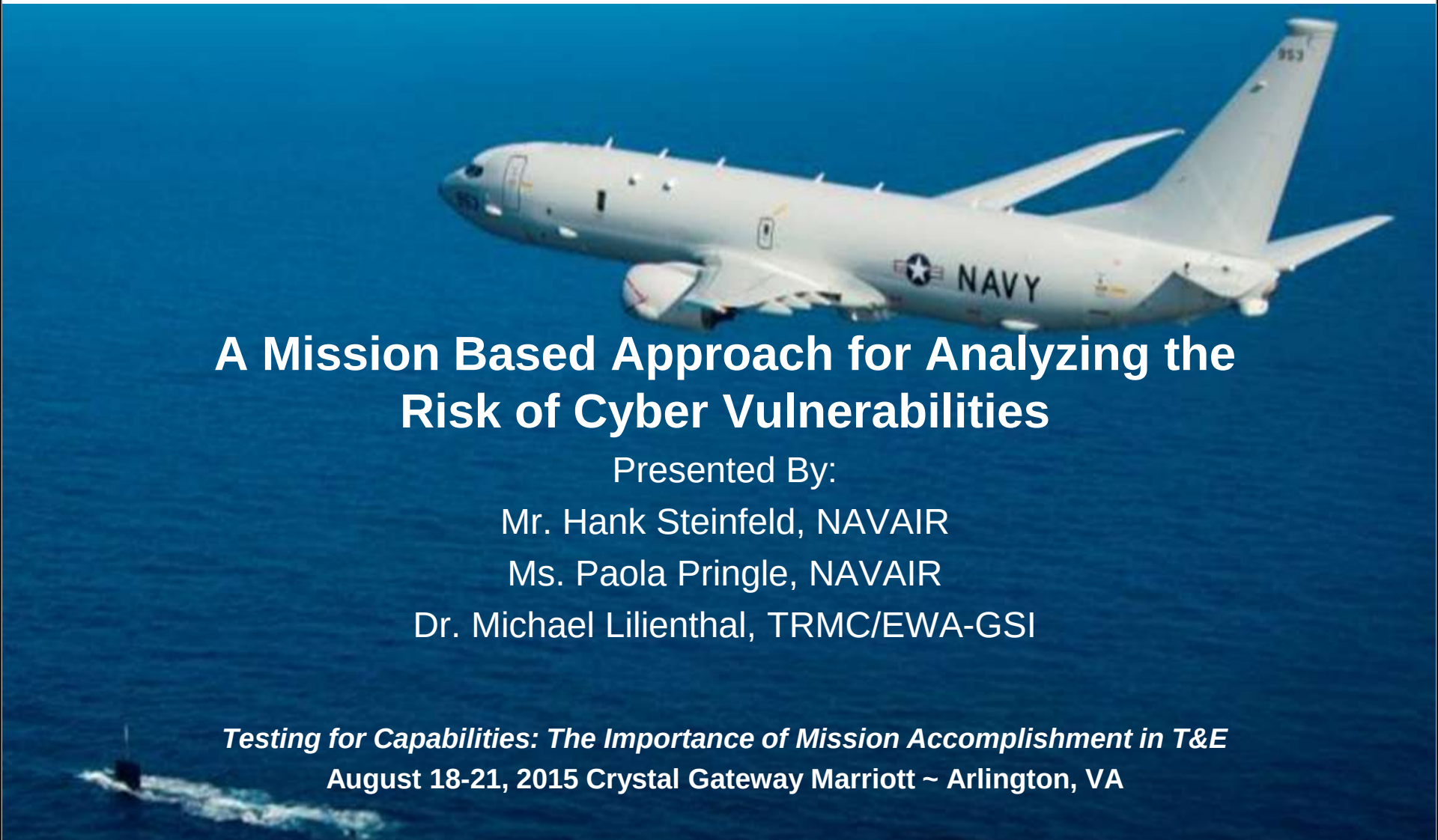


A Mission Based Approach for Analyzing the Risk of Cyber Vulnerabilities

Presented By:

Mr. Hank Steinfeld, NAVAIR

Ms. Paola Pringle, NAVAIR

Dr. Michael Lilienthal, TRMC/EWA-GSI

Testing for Capabilities: The Importance of Mission Accomplishment in T&E

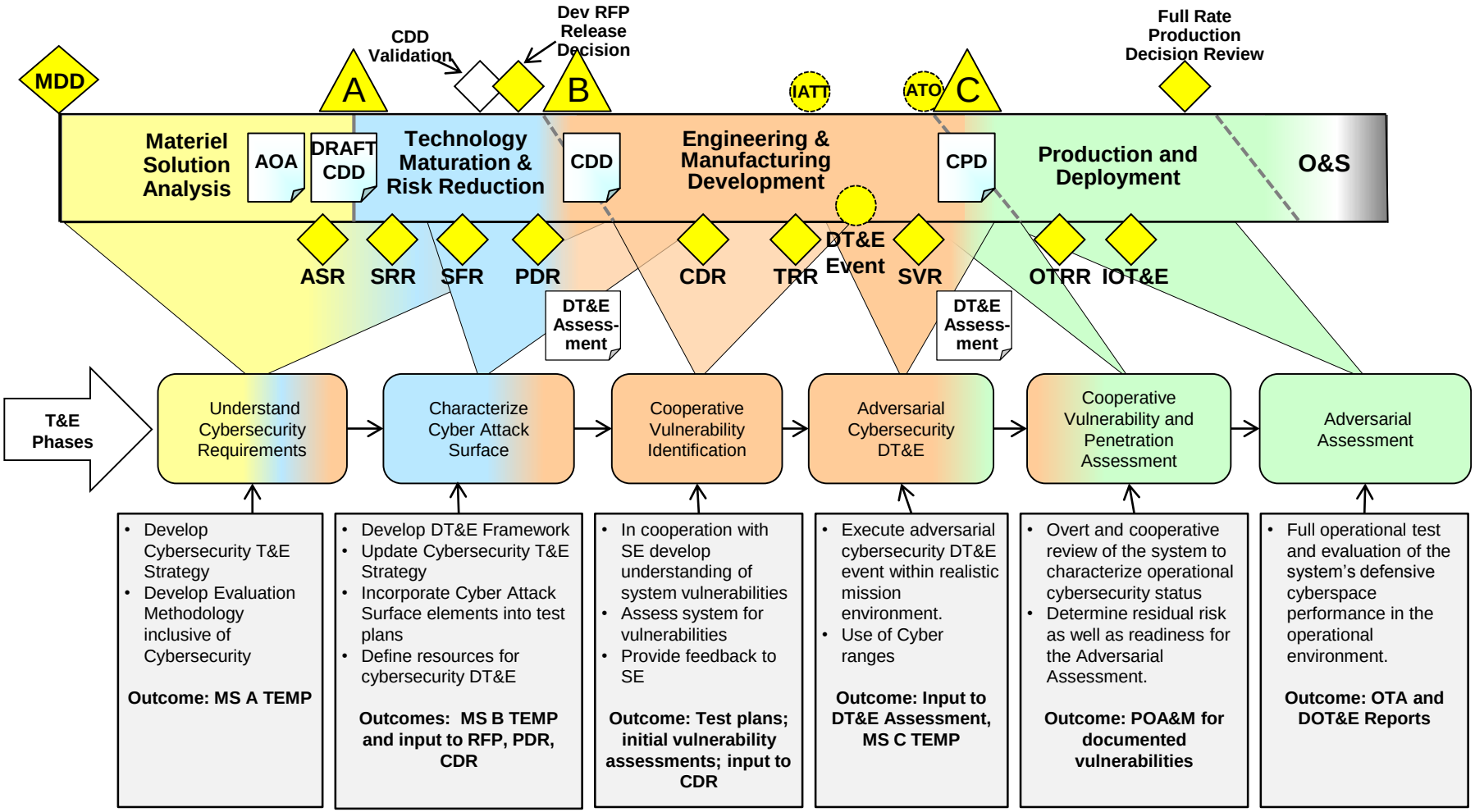
August 18-21, 2015 Crystal Gateway Marriott ~ Arlington, VA

Why are we here?

- **Yes! Every communication path represents a risk to security**
  - Each being vulnerable to cyber attack
- **No! Existing reports do not offer all the answers we need**
- **No! Our budgets cannot sustain testing every single communication path that goes in to or out of our platforms**
- **Yes! Methods need to be developed to determine what is and is not a risk to security**
- **Yes! Need to consider low cost methods to assess what areas are highest risk**
- **Questions:**
  - How likely is an attack to succeed in accomplishing it's mission?
  - And if likely, how much of an impact will it have in accomplishing the mission?

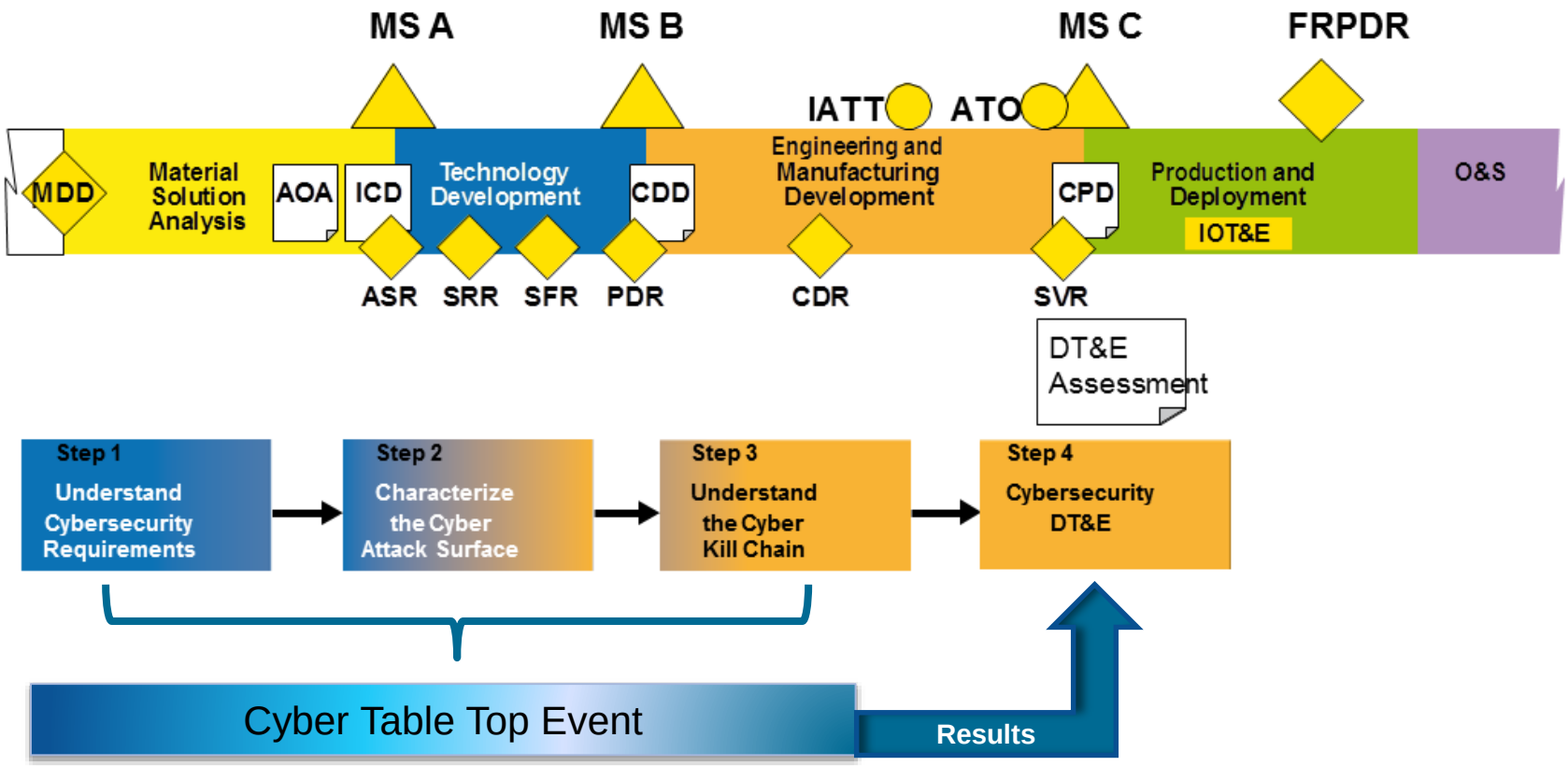
Need to 'right size' testing
To identify what's most important

OT&E Six Steps to Cybersecurity

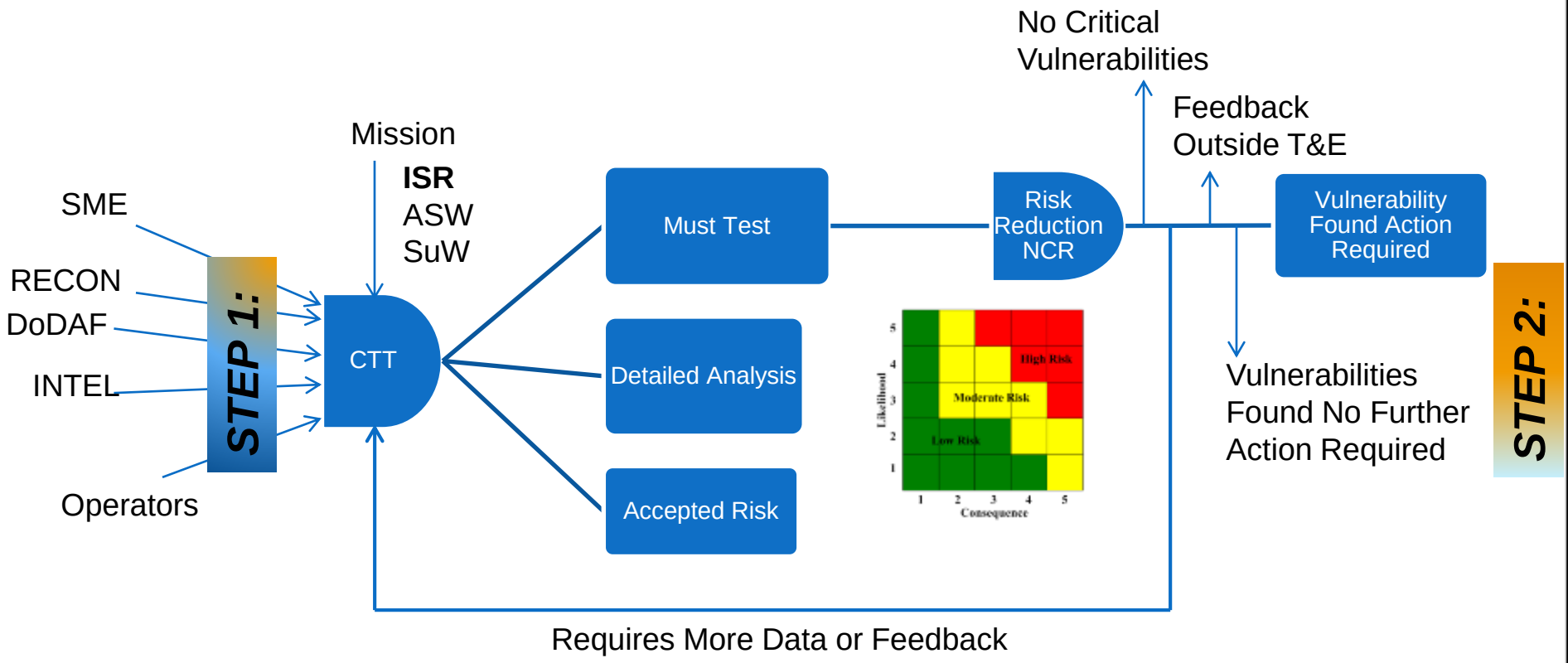


Phases are iterative and executed as part of the Acquisition continuum.

DT&E Four Steps to Cybersecurity



An Approach to the Cyber Test Strategy



STEP 1: CTT

CTT Process

PHASE 1 Event Preparation

- Analyze DoDAF, CONOPS, RECON, INTEL
- Define entry criteria, scenario, blue and red mission
- Identify Control, Red, Blue, Analysis, & Reporting Teams

PHASE 2 Event Execution

- System exposure to common vulnerabilities
- Attack Surface – likely avenues of cyber-attack

PHASE 3 Post Mission Analysis

- Determine effects of cyber-attacks (FMC, PMS, NMC)
- Determine likelihood of successful attack
- Determine consequence of successful attack

PHASE 4 Reporting

- Document risk cubes
- Executive Briefing
- Detailed Briefing
- Full Report

Phase 1: Event Preparation

It's All About the People

- **Operators**
- **Assistant Program Manager for T&E**
- **Test and Evaluation Engineers**
- **Systems Engineers**
- **Subject Matter Experts**
- **Interoperability Engineers**
- **Certified Ethical Hackers**
- **Red Team Members**
- **Blue Team Members**
- **Data Collection Team**

Select Your Operational Scenario

Transformational Mixed Force: Effective, Efficient Mission Capability Tailored to the Warfighter's Requirements

Responsive Multi-Mission

- Robust Sensor Suite
- Cue to Kill
- Onboard Fusion
- Large Weapons Payload

Persistent ISR

- Long Dwell Sensor Suite
- C4I Network Node (FORCEnet)
- Combat Info from MCS
- Data Available to Intel Centers
- High Altitude, Fast, Reliable

ASW Kill
ASW Track
ASW Search

SuW Kill

SuW Classify/ID
SuW Track
SuW Detect

Maintain Maritime COP

FRP Tripwire

ISR in Support of IPE

Navy Maritime Patrol Missions

Phase 2 Event Executions

Day 1

Event Execution

Develop Mission Plan

Establish:

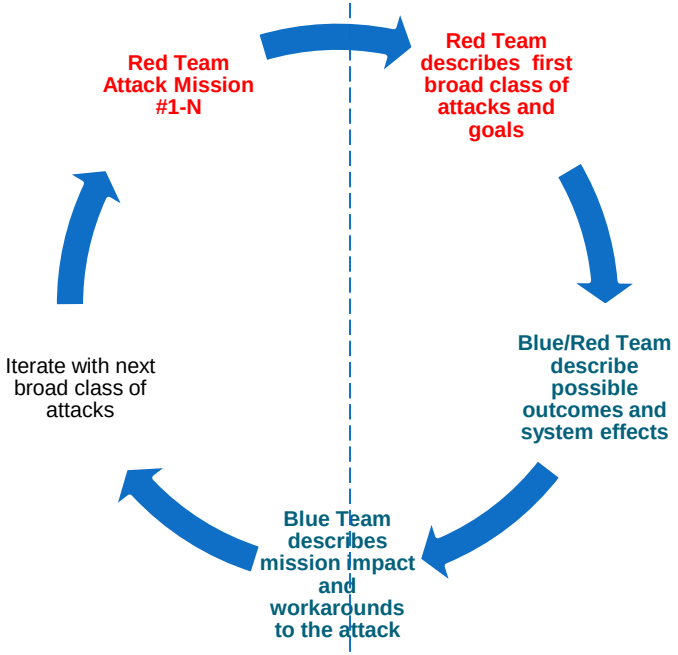
- ***Purpose***
- ***Goals***
- ***Expected Output***
- ***Blue Team Mission Order***

Examine Attack Surface

Day 2

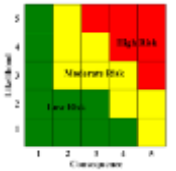
Blue & Red Team Briefs

Red Team Mission Orders #1-#N



Day 3

Post Mission Analysis

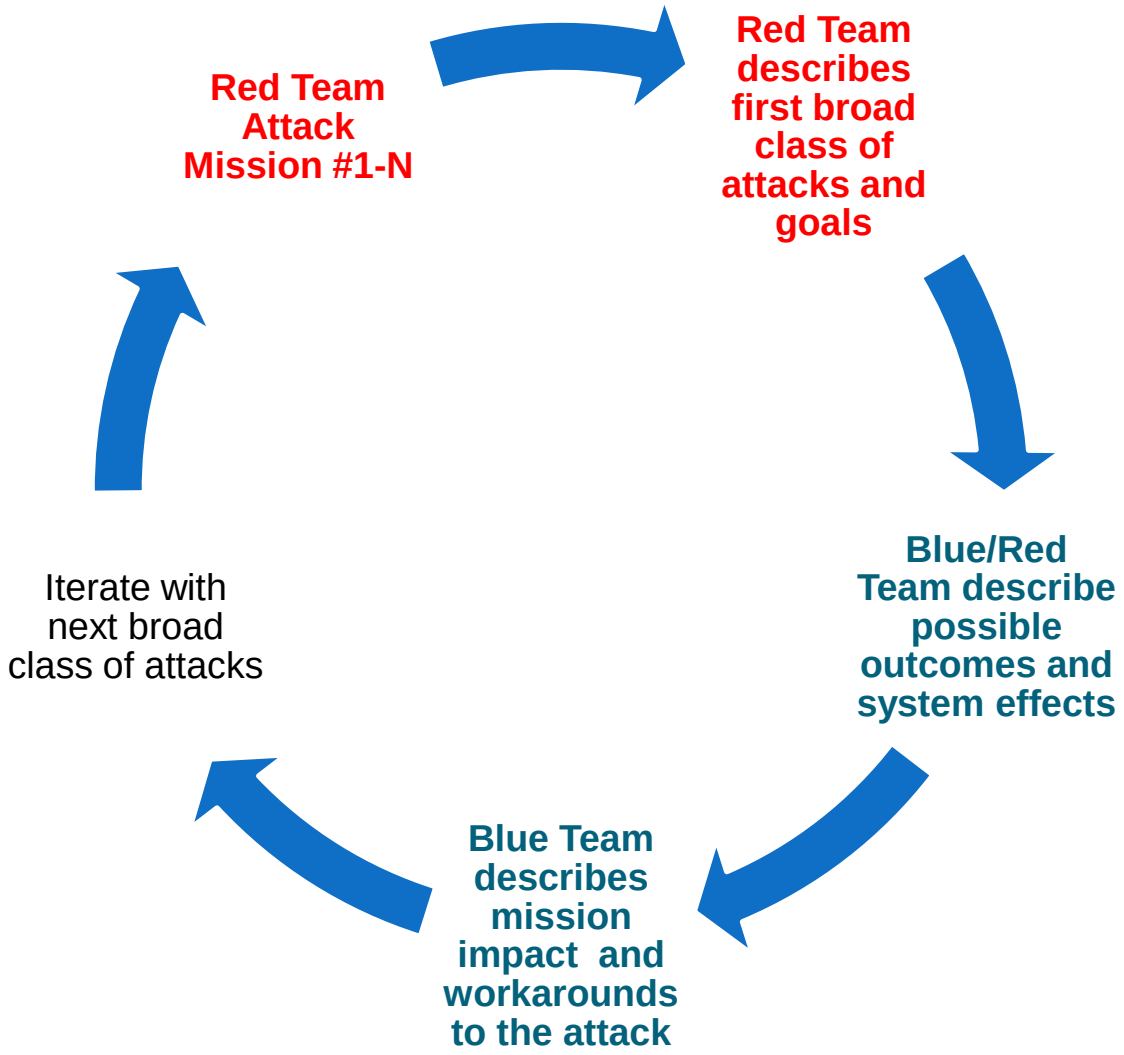


Color Code

Operational (Blue) Team

Opposing Force (Red) Team

Blue/Red Team Collaboration



Phase 3: Post Mission Analysis

Adversary or OPFOR Team Lead			
Attack Method	**Attack Goal**	**Assumptions**	**When in the Mission Timeline**
Attack Type 1	Attack Type 1 Variant 1		
	Attack Type 1 Variant 2		
	Attack Type 1 Variant 3		
Attack Type 2	Attack Type 2 Variant 1		
	Attack Type 2 Variant 2		
	Attack Type 2 Variant 3		

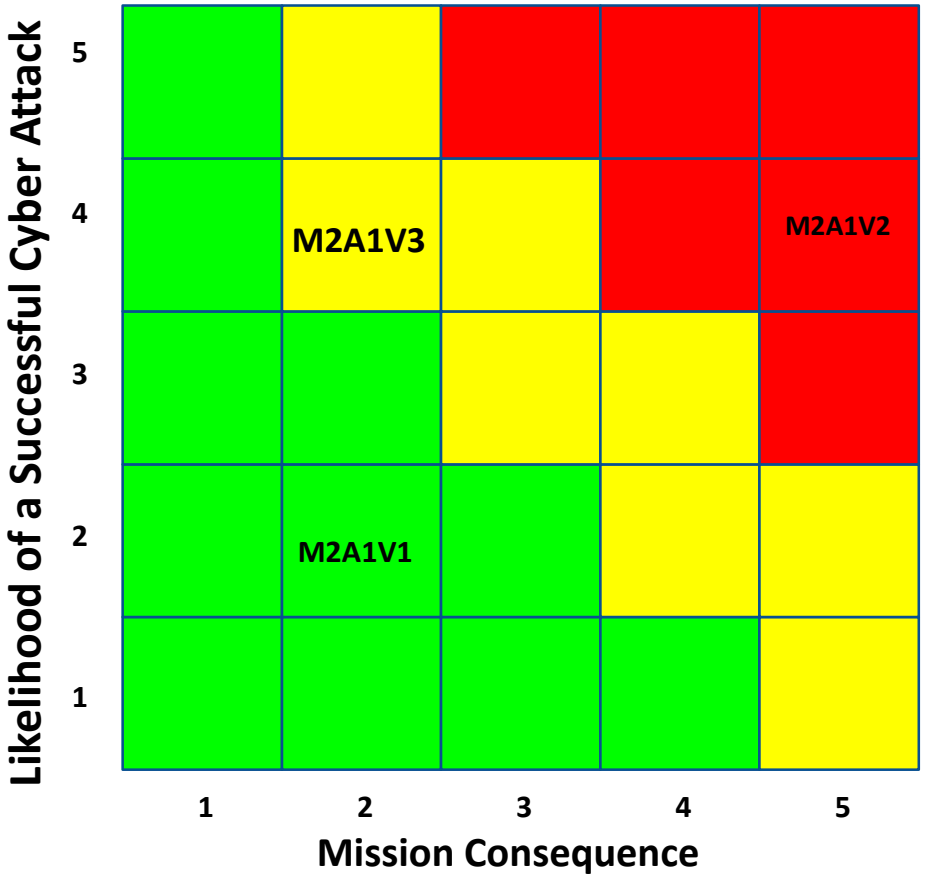
White Team Lead		Operational Blue Team Leads		White Team Lead	
Possible Outcome	**Attack Result**	**Mission Impact**	**Mission Consequence**	**Attack Cost / Level of Effort**	**Attack Success Likelihood**
System / Subsystem 1					
System / Subsystem 2					
System / Subsystem 1					
System / Subsystem 3					
System / Subsystem 2					
System / Subsystem 3					
System / Subsystem 1					
System / Subsystem 2					
System / Subsystem 1					
System / Subsystem 3					
System / Subsystem 2					
System / Subsystem 3					

System Test Leads		
System's Information Assurance & Cyber Security Mechanisms		Recommendations
In Place Today	Planned for the Future	

Notional Risk Assessment

How likely is the attack to result in it's intent?

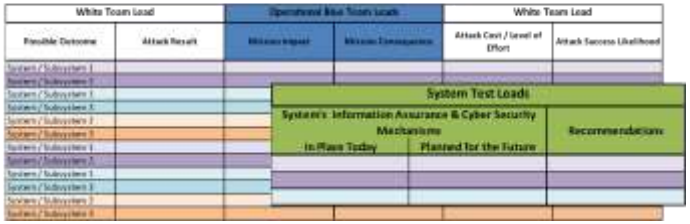
Fully,
Partially, or
Not successful

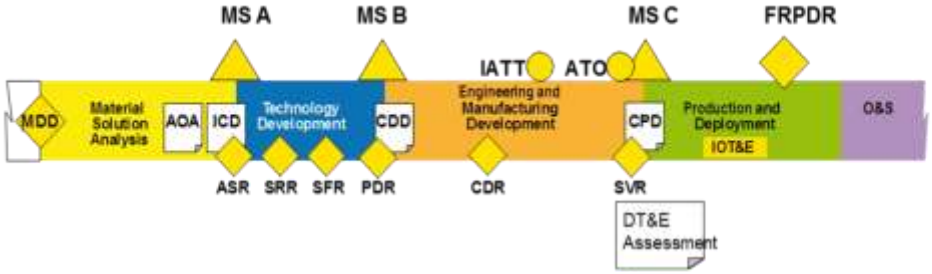


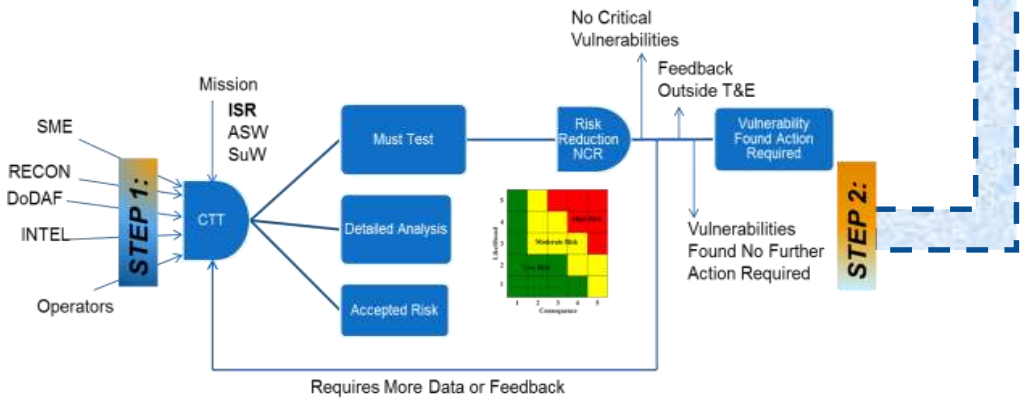
M = Mission
A = Attack
V = Variant

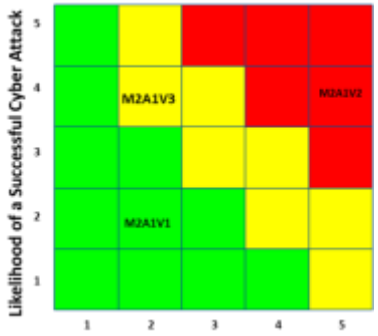
What impact is there to your mission?
full, partial, or non-mission capable

Step 3 Understood









Development testing is now 'right sized'
What's most important has been established

Questions

Contact Information

Hank 'Wizard' Steinfeld, FIAE PMA-290/PMA-264
APM T&E, P-8A Inc 3, P-3C, EP-3E
APM T&E MAC, HAASW
301-342-3041
henry.steinfeld@navy.mil

Ms. Paola Pringle
Integrated Warfare Test and Evaluation Division, 5.1L
Cyberspace T&E Branch 51L300E
P-8A Increment 3 Interoperability LTE
(805) 816-3038 main
paola.pringle@navy.mil

Michael G Lilienthal PhD CPE CBP
Joint Mission Environment Test Capability (JMETC) Office Support to Deputy for Operations Planning
571-238-4532
Michael.g.lilienthal.ctr@mail.mil
MLilienthal@ewa.com