How to Accomplish a Cyber Table Top

MEGAN FISHER

JT4/ATAC

812 AITS/ENIE

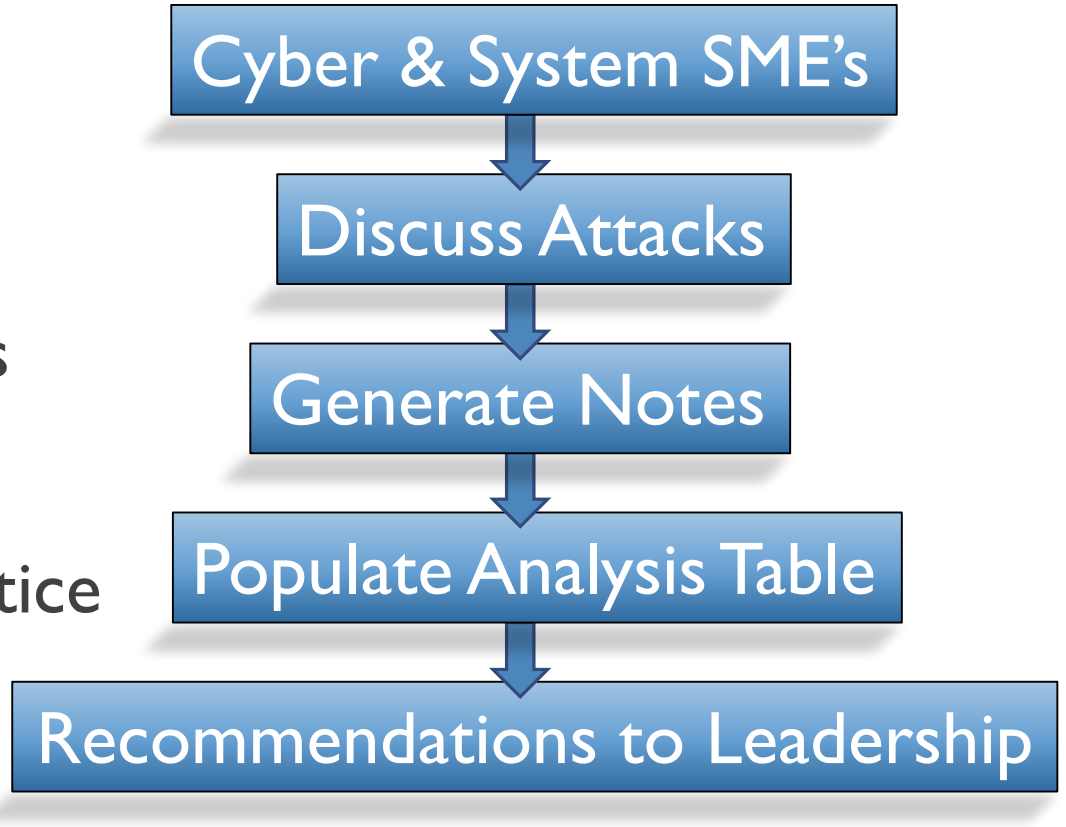
MAY 2019

CTT Philosophy

WHAT IT IS AND WHEN TO USE IT

Benefits of the Cyber Table Top

- Customizable
- Discussion Based (no hardware)
- Methodical & Analytical
- Help Leadership Allocate Resources
- Community Involvement
- Closing Gap Between Policy & Practice



Benefits of the Cyber Table Top

- Customizable
- Discussion Based (no hardware)
- Methodical & Analytical
- Help Leadership Allocate Resources
- Community Involvement
- Closing Gap Between Policy & Practice

Edwards AFB Instrumentation CTT

50 People

89 Attacks

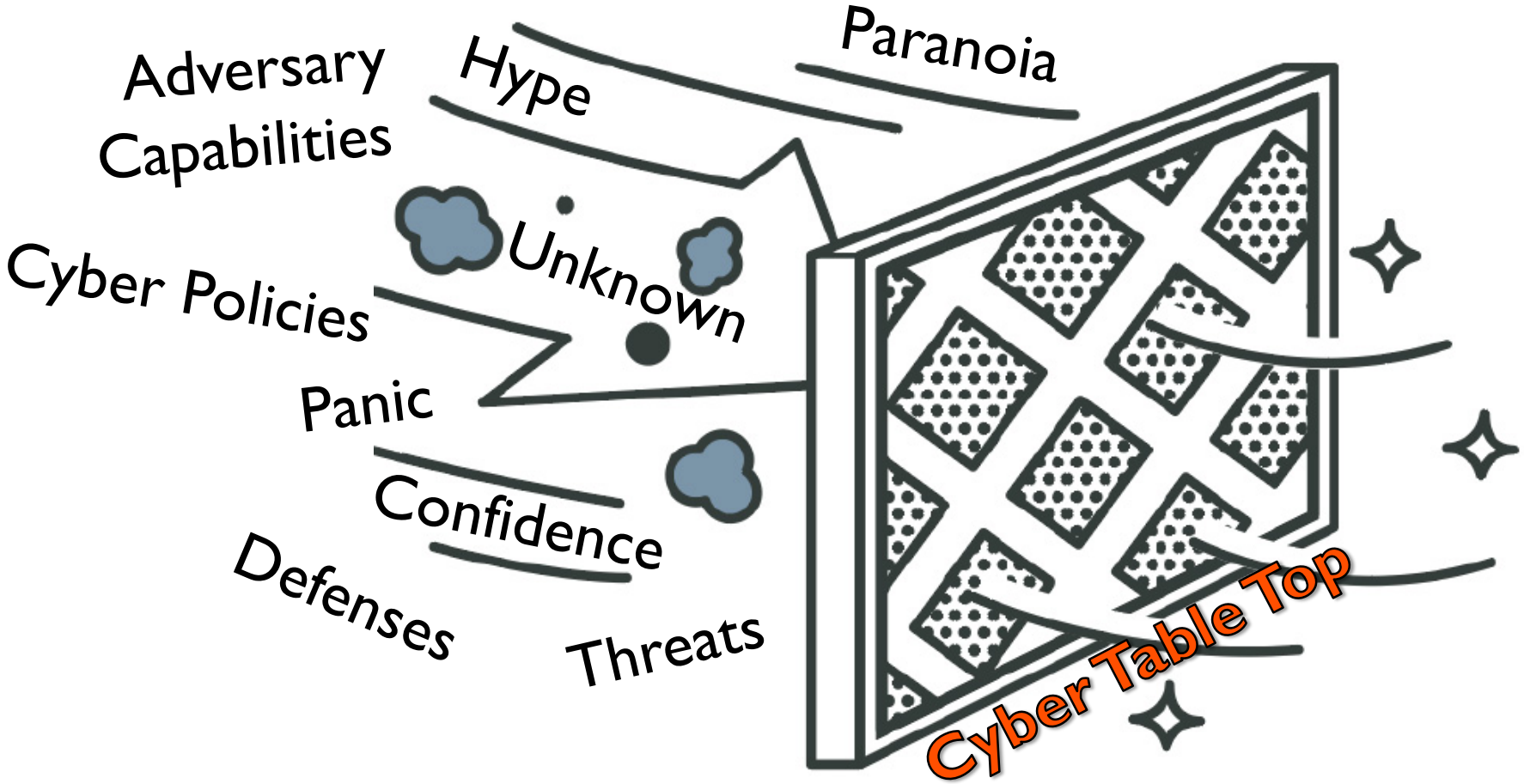
450 Pages of Notes

1 Massive Analysis Table

20 Categories of Recommendations

Closing the Gap Between Policy & Practice

Analytical (Filtering Hype)



Technically feasible threats that adversely impact the mission.

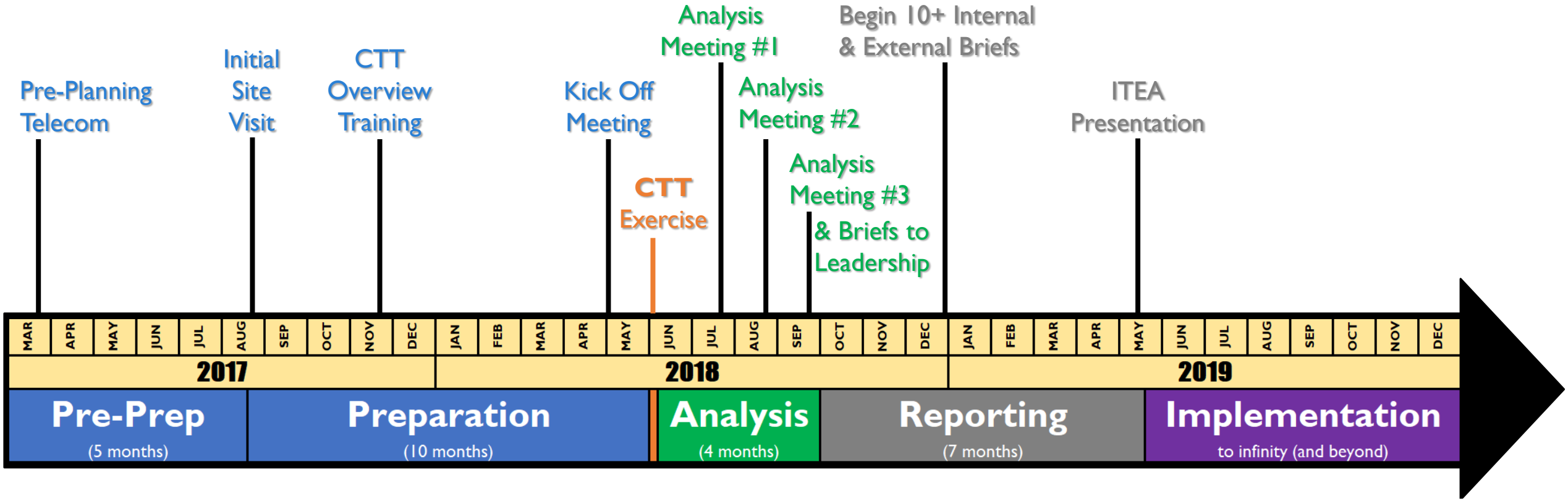
CTT Process

4 PHASES, 3 TEAMS

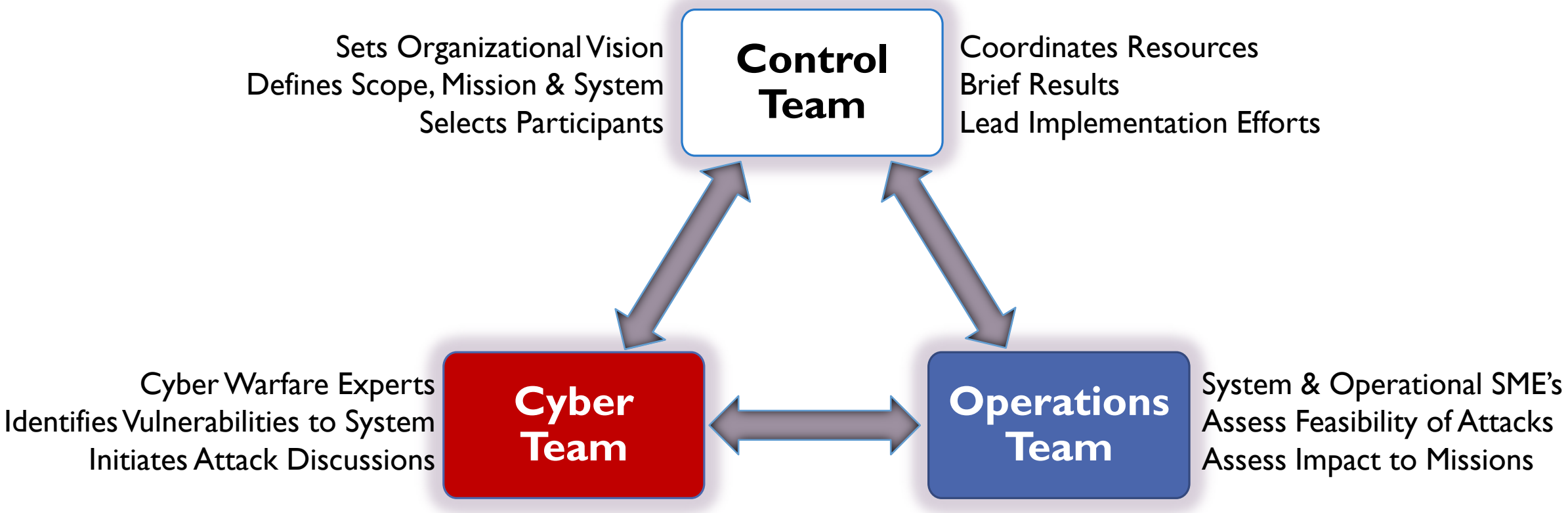
CTT Phases

Exercise Preparation	Exercise Execution	Post Exercise Analysis	Reporting
Understand Organizational Goals	Review SCG, Logistics & Admin	Analysis Meeting #1: Review Exercise	Brief to Internal Leadership
Define System & Operational Mission	Describe System, Mission & Scope	Analysis Meeting #2: Complete Table	Brief to Internal Community
Select Boundaries and Participants	Discuss Cyber Missions & Attacks	Analysis Meeting #3: Develop Briefs	Brief to External Organizations

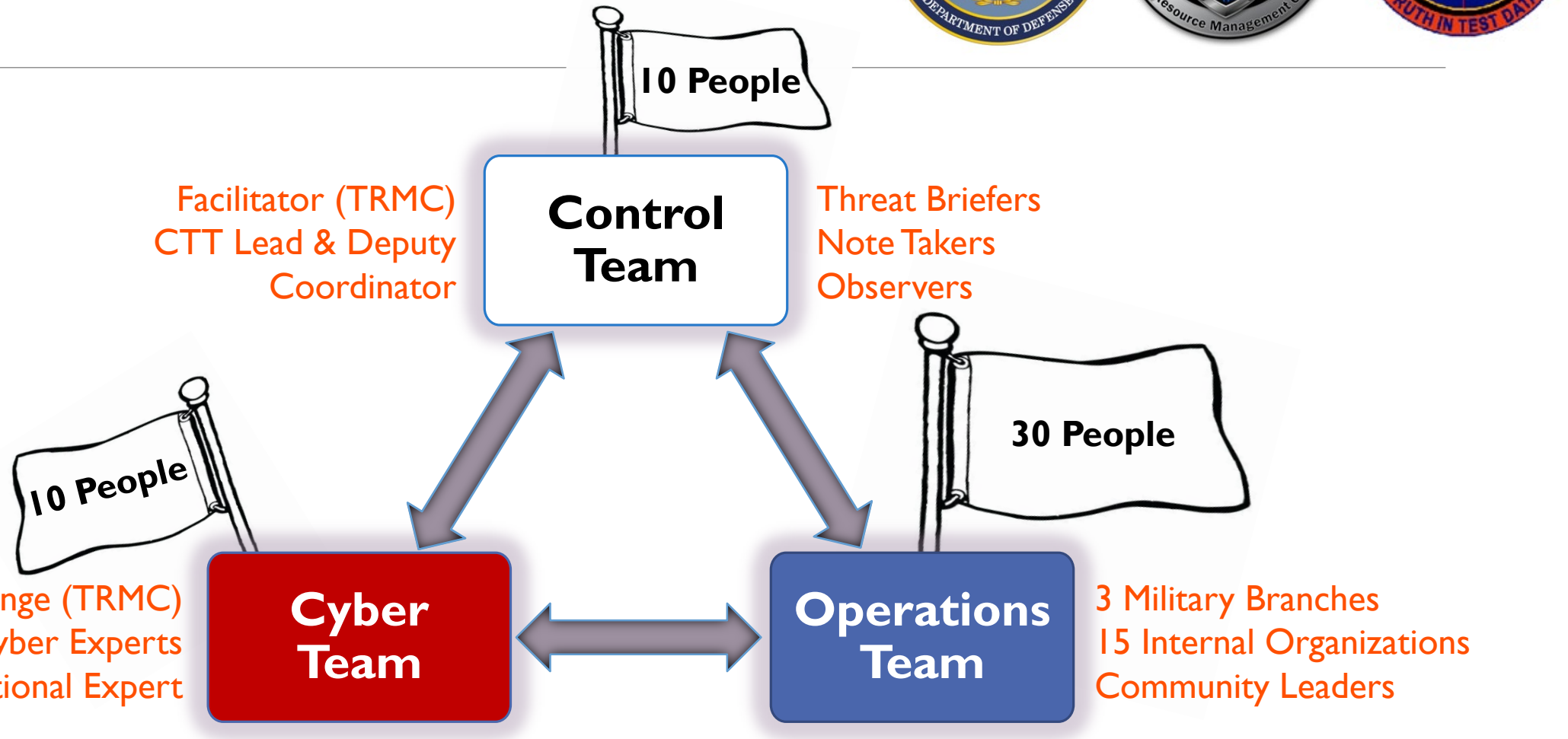
CTT Phases


Pre-Planning Telecom
Initial Site Visit
CTT Overview Training
Kick Off Meeting
CTT Exercise
Analysis Meeting #1
Analysis Meeting #2
Analysis Meeting #3 & Briefs to Leadership
Begin 10+ Internal & External Briefs
ITEA Presentation
MAR APR MAY JUN JUL AUG SEP OCT NOV DEC JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC JAN FEB MAR APR MAY JUN JUL AUG SEP OCT NOV DEC
2017
2018
2019
Pre-Prep
(5 months)
Preparation
(10 months)
Analysis
(4 months)
Reporting
(7 months)
Implementation
to infinity (and beyond)

CTT Players


Sets Organizational Vision
Defines Scope, Mission & System
Selects Participants
Control Team
Coordinates Resources
Brief Results
Lead Implementation Efforts
Cyber Warfare Experts
Identifies Vulnerabilities to System
Initiates Attack Discussions
Cyber Team
Operations Team
System & Operational SME's
Assess Feasibility of Attacks
Assess Impact to Missions

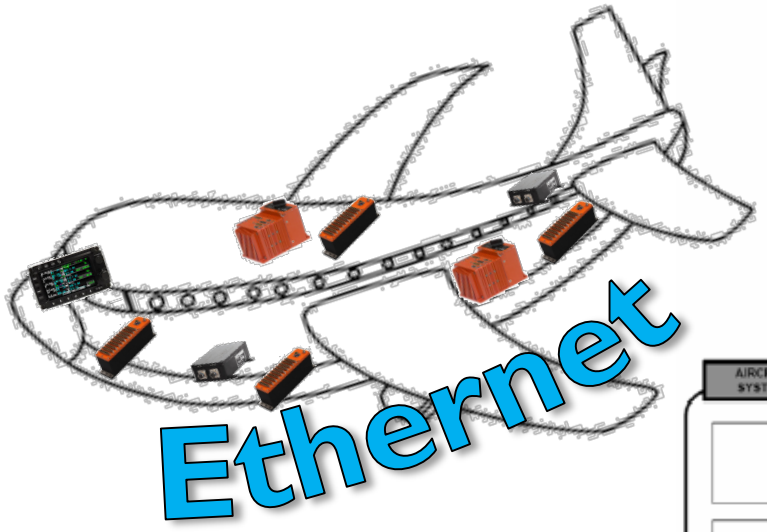
CTT Players

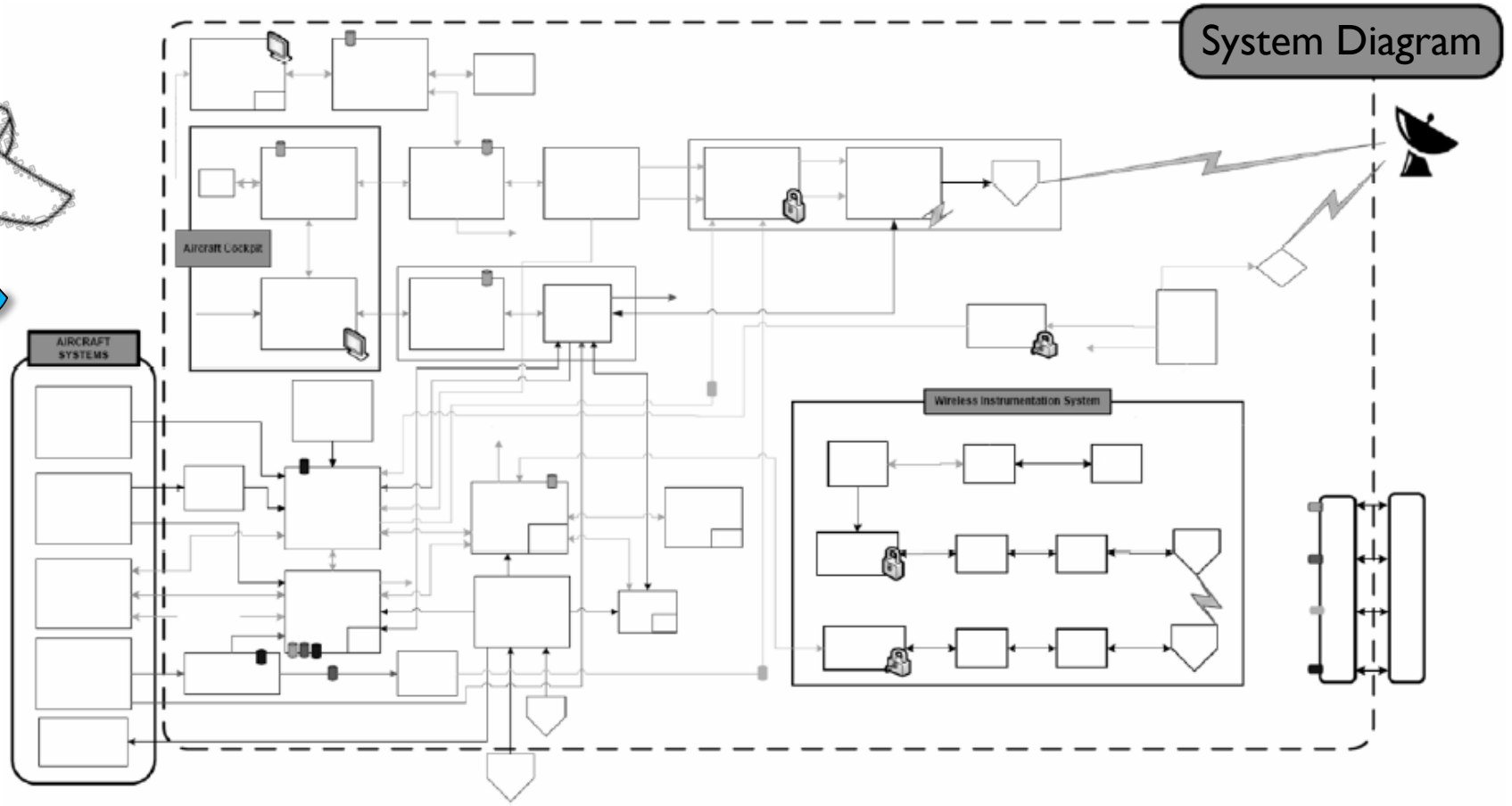

10 People
Facilitator (TRMC)
CTT Lead & Deputy
Coordinator
Control Team
Threat Briefers
Note Takers
Observers
10 People
30 People
National Cyber Range (TRMC)
Internal Cyber Experts
Operational Expert
Cyber Team
Operations Team
3 Military Branches
15 Internal Organizations
Community Leaders

Exercise Preparation

SYSTEM, MISSION AND PARTICIPANTS

System Definition





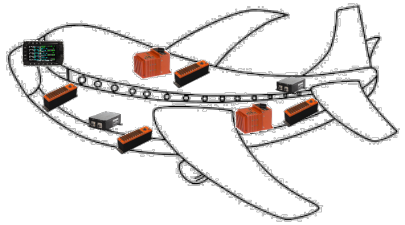
Mission Description

Procurement | Design | Install | Operations | Maintenance

Offices

Test Equipment

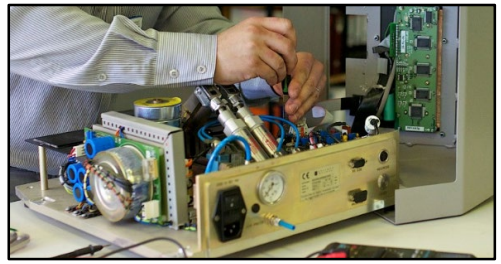
Labs



Mod Dock

Check Out Vehicles

Hangars
Flight Line



Vendors

Boundary Determination

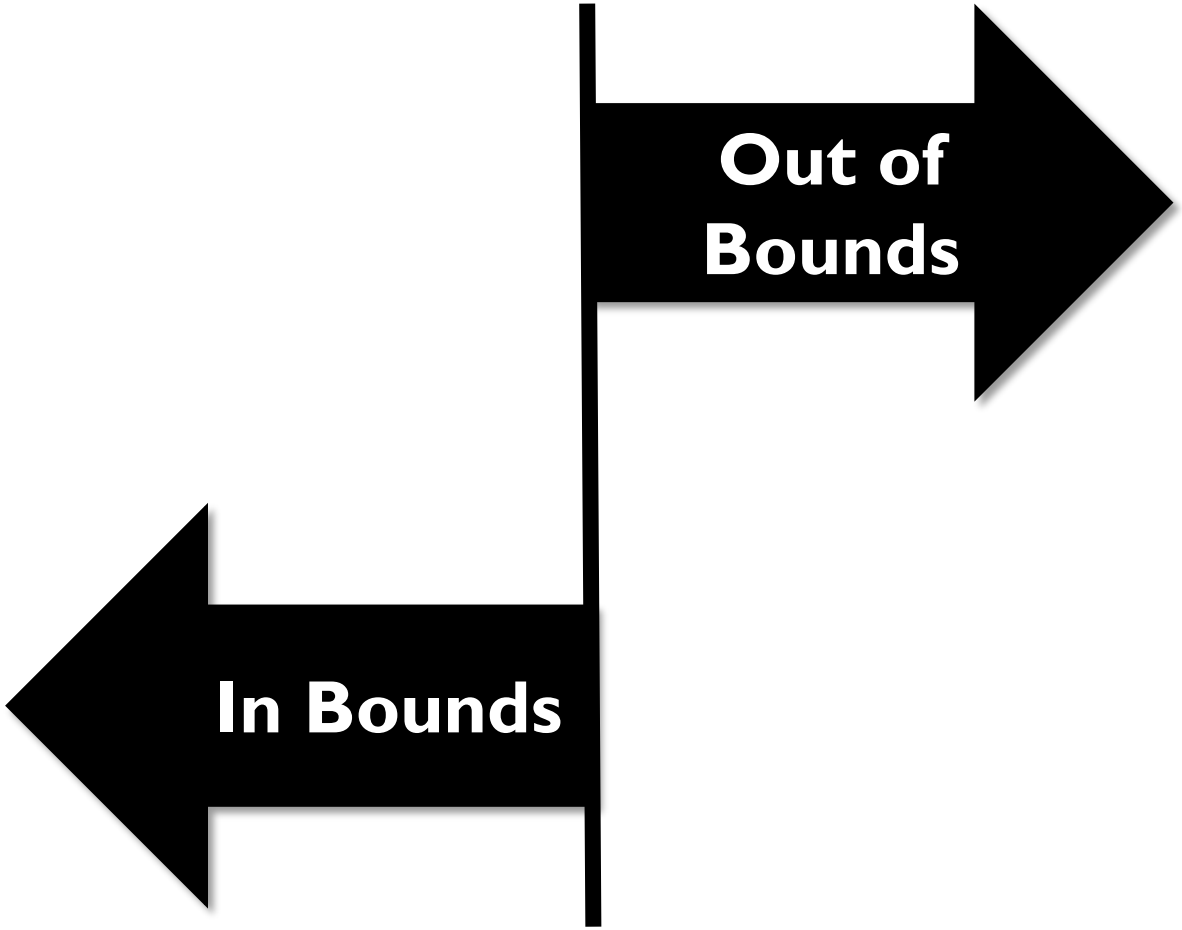
Procurement

Design

Install

Operations

Maintenance



Production Aircraft
Control Rooms
Vendor Facilities

Type I Encryption
TmNS & iNet
Wireless

Participant Selection

Procurement

Program Managers
Procurement Specialists

Design

Design Engineers
Software Developers
RF Engineers
Lab Technicians
Electrical Technicians

Install

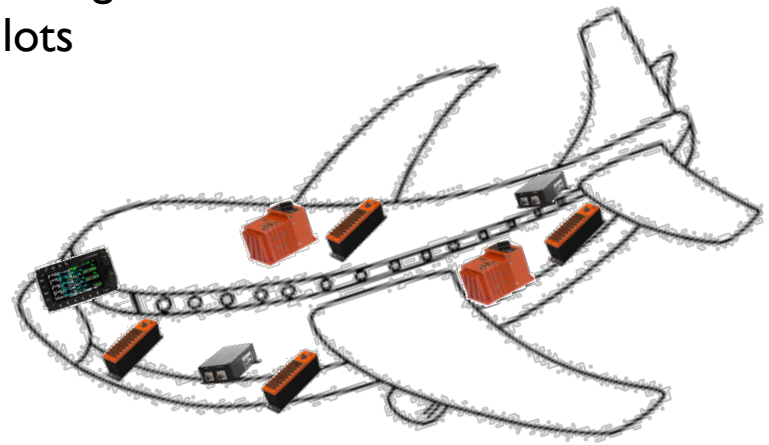
Aircraft Technicians
Mechanical Technicians
Electrical Technicians

Operations

CTF Leads
Aircraft Technicians
Operations Engineers
Pilots

Maintenance

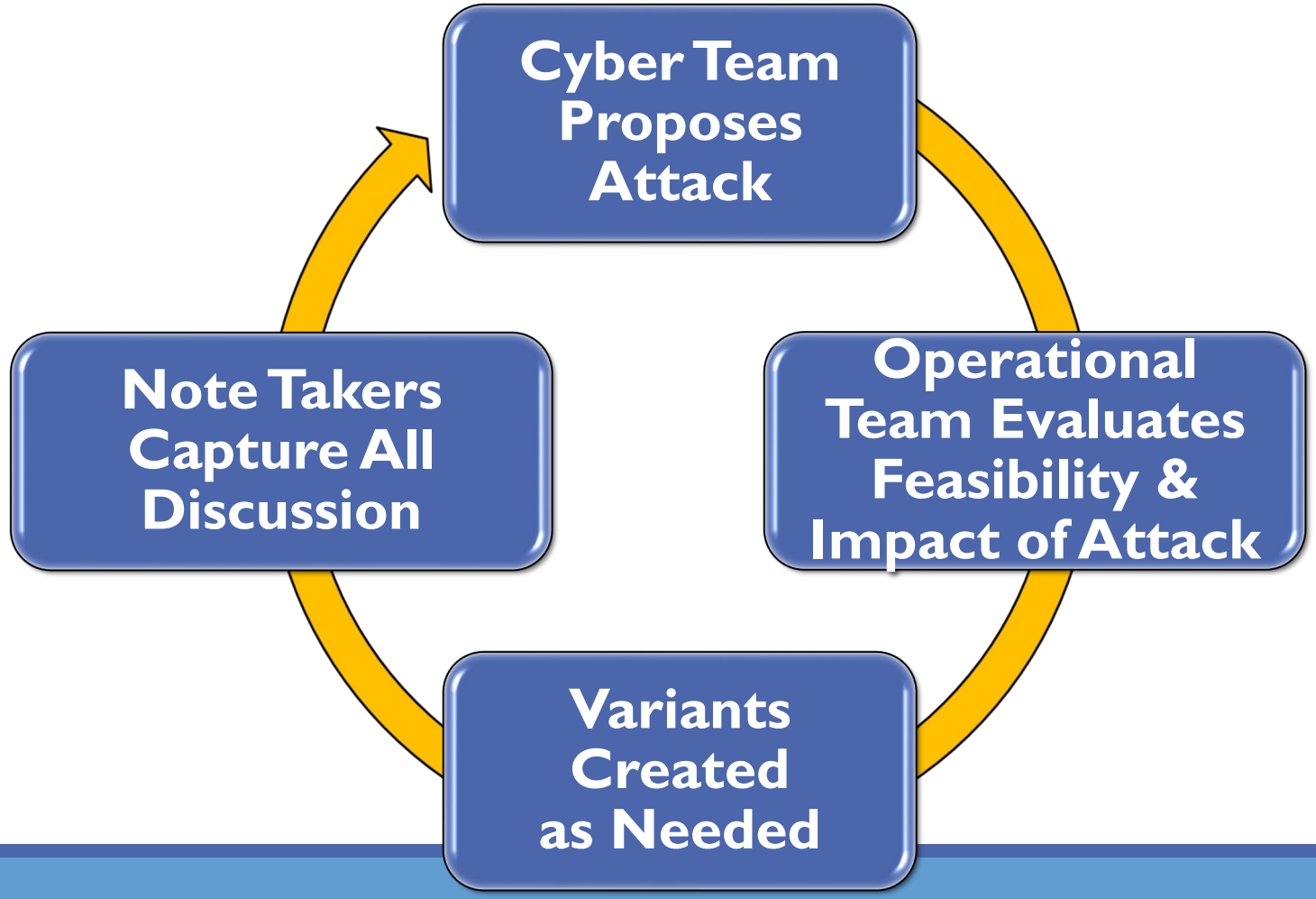
Logisticians



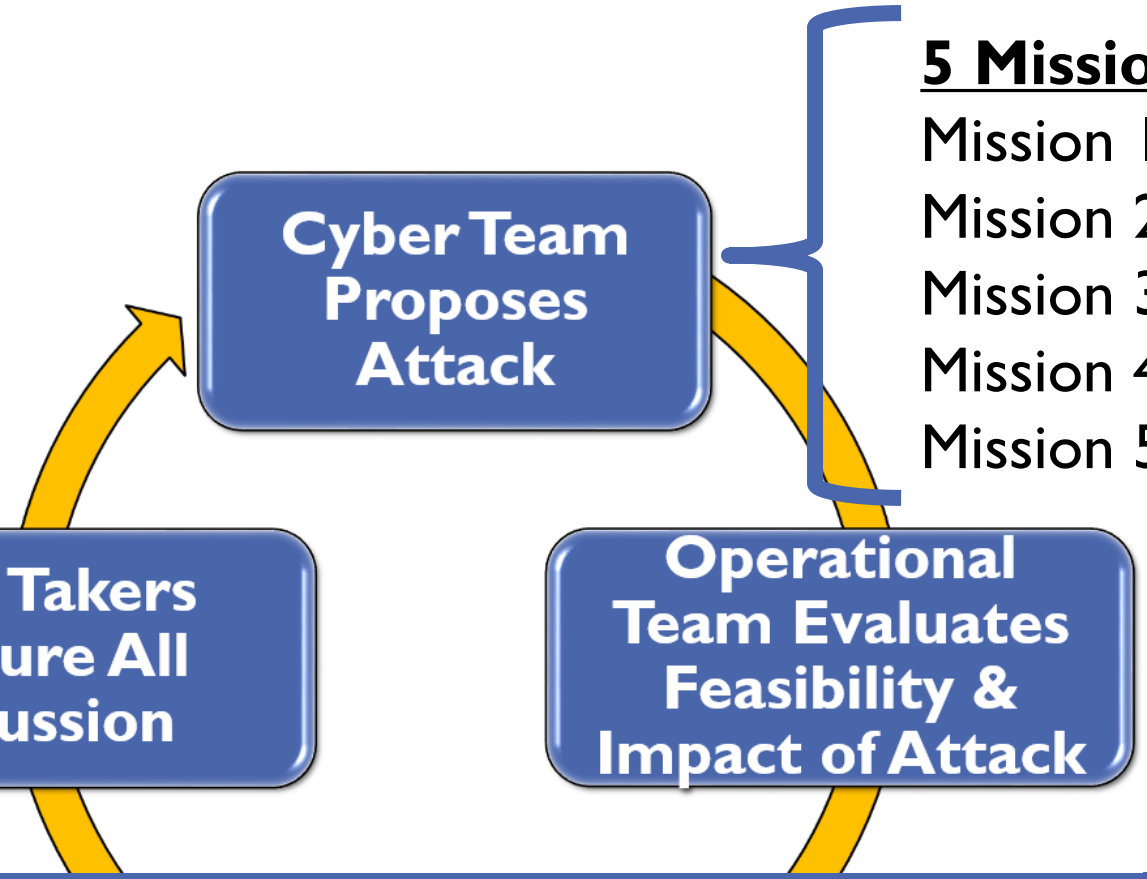
Exercise Execution

NOT A TRADITIONAL WARGAME

Exercise Process



Exercise Missions



5 Missions (89 Attacks)

Mission 1: Gain Access (41 attacks)

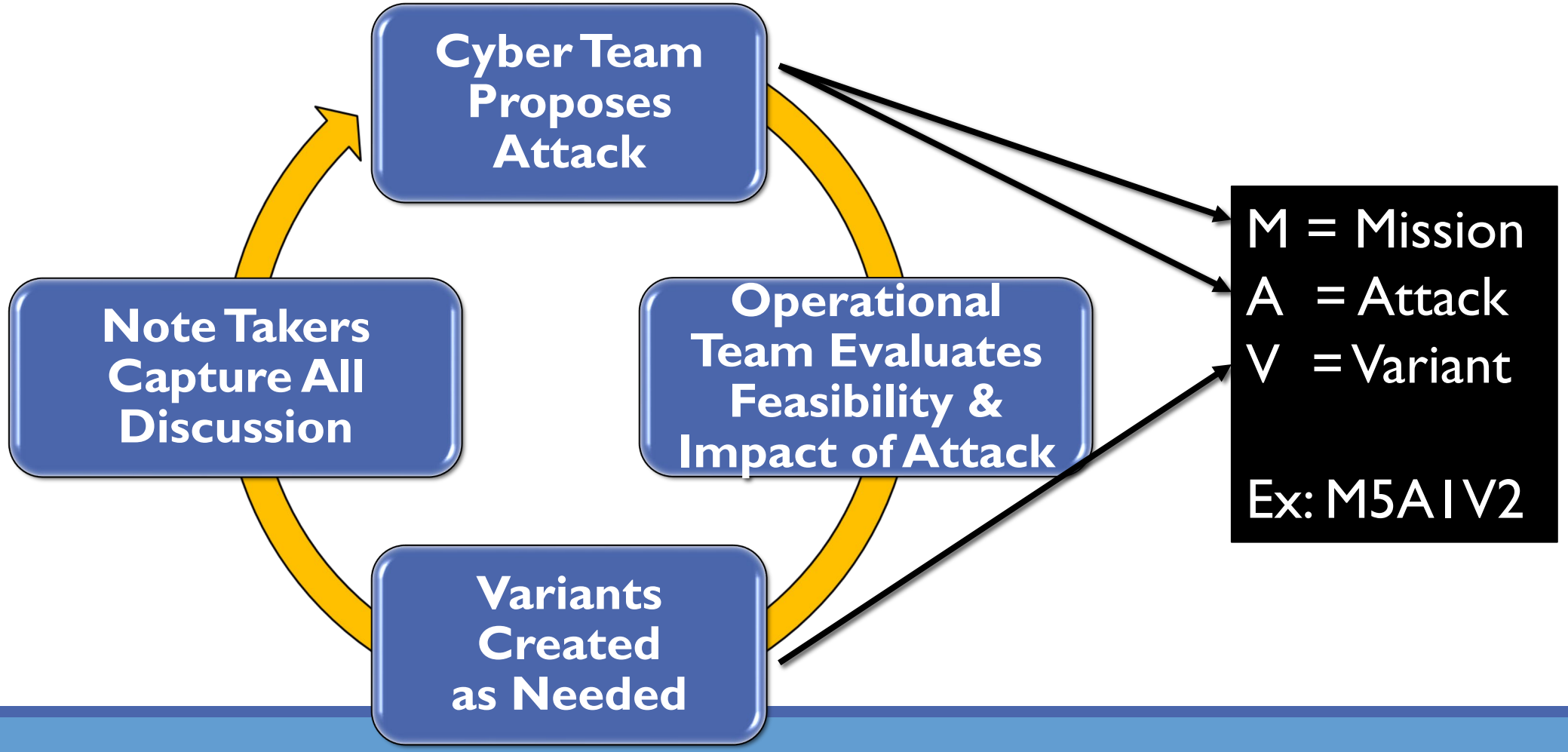
Mission 2: Disrupt Testing Operations (14 attacks)

Mission 3: Disrupt Instrumentation System (13 attacks)

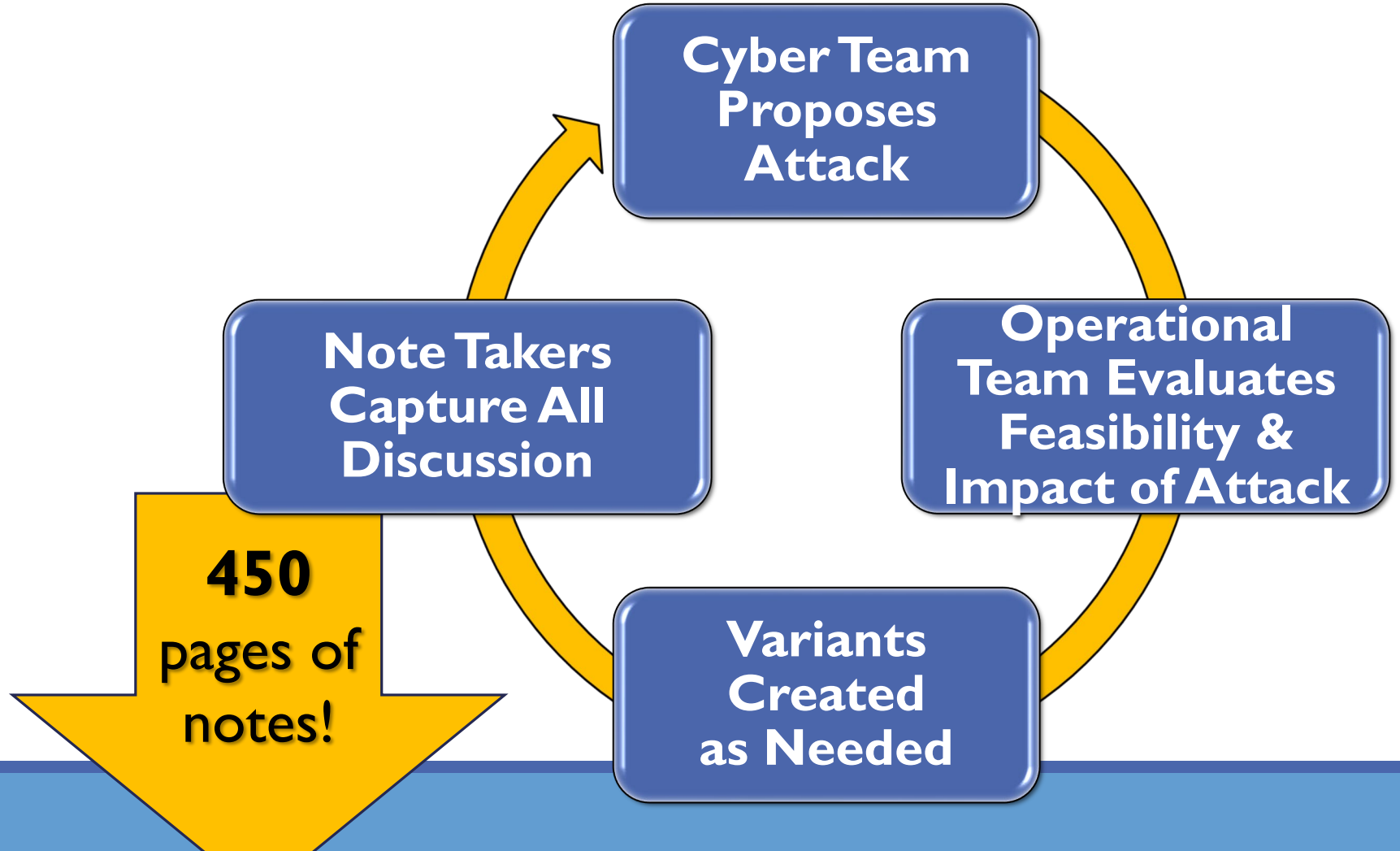
Mission 4: Corrupt, Destroy or Modify Test Data (15 attacks)

Mission 5: Exfiltrate Test Data (6 attacks)

Exercise MAV's



Exercise Notes



Post-Exercise Analysis

ORGANIZING & ASSESSING THE INFORMATION

Analysis Table

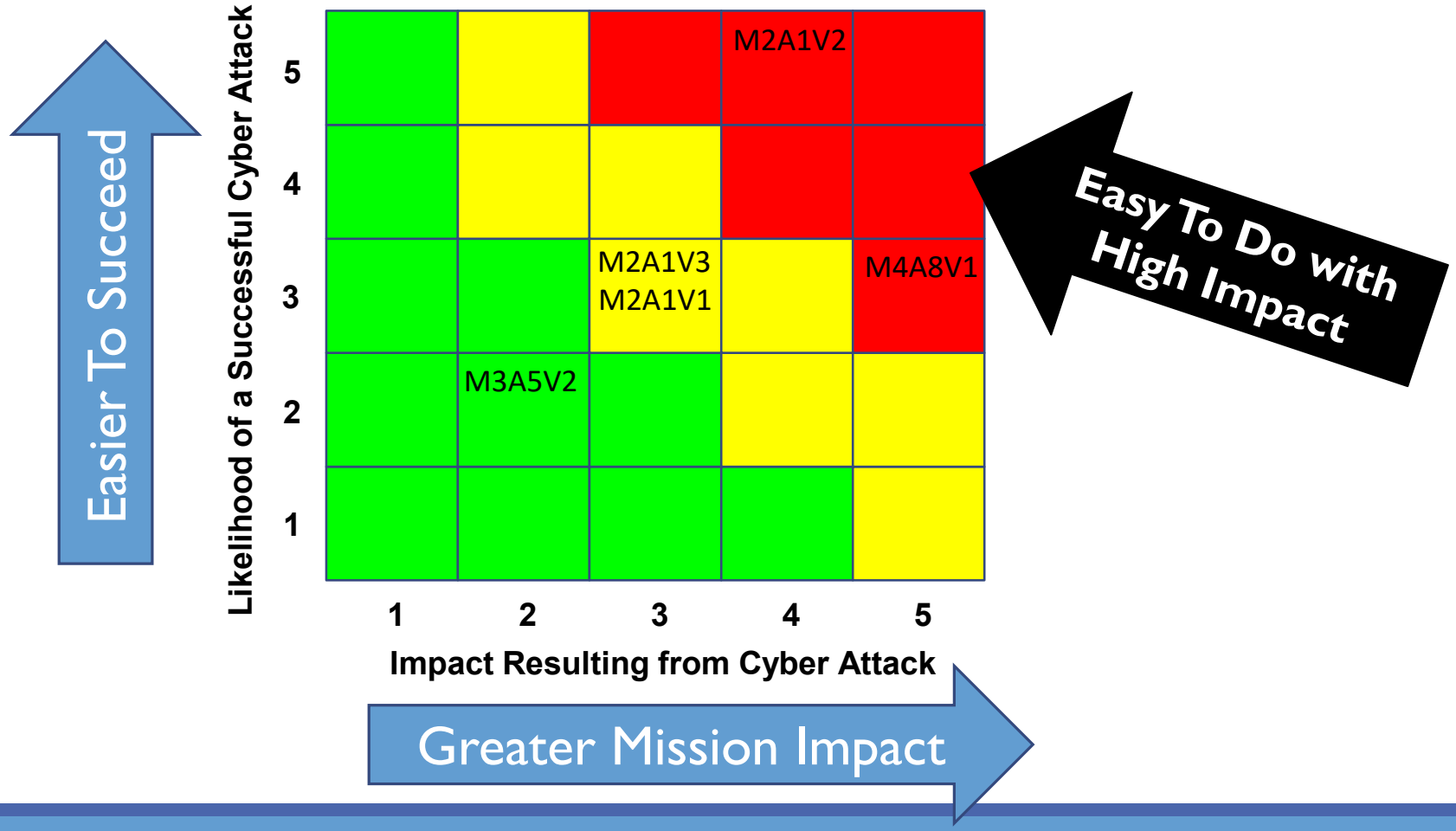
Mission Attack Variant

	OPFOR				Control Team/ OPFOR		Operational Team	
ID	Goal	Attack Method Attack Description	Assumptions	When in the Mission Timeline	Possible System Effect (IF)	Attack Result (THEN)	Mission Effect (IF)	Misson Impact (THEN)
M1A1V1								
M1A1V2								

Goal

Analysis Team					
Numerical Mission Impact and Consequence	Attack Cost / Level of Effort	Attack Success Likelihood	Numerical Likelihood	Analysis of numerical Likelihood factoring in access methods. Put new (or unchanged) likelihood value from N.	Final Risk Assessment coordinates

Analysis Risk Matrix



Analysis: Mission Impact

The impact of each attack is evaluated using a Mission Impact Methodology chart.

Impact	Mission Impact	Data Loss (MEF)	System Performance (MEF)	Delay (Operational Mission)
1	Fully Mission Capable	No data compromised	System Performance Not Impacted	Less than 5 Minutes
2	Partial to Fully Mission Capable	Public Access Level	System Performance Marginally Impacted	Greater than 5 Minutes and less than 30 Minutes
3	Partially Mission Capable	FOUO	Partial Loss of Functionality	Greater than 30 Minutes and less than 1 Hour
4	Non to Partially Mission Capable	FOUO/New Technology	Major Loss of Functionality	Greater than 1 Hour, less than 2.5 Hours
5	Non-Mission Capable	Classified	System Performance Severely Impacted/ Total Loss of Functionality	Greater than 2.5 Hours

Analysis: Mission Impact

Impact	Mission Impact	Data Loss (MEF)	System Performance (MEF)	Delay (Operational Mission)
1	Fully Mission Capable	No data compromised	System Performance Not Impacted	Less than 5 Minutes
2	Partial to Fully Mission Capable	Public Access Level	System Performance Marginally Impacted	Greater than 5 Minutes and less than 30 Minutes
3	Partially Mission Capable	FOUO	Partial Loss of Functionality	Greater than 30 Minutes and less than 1 Hour
4	Non to Partially Mission Capable	FOUO/New Technology	Major Loss of Functionality	Greater than 1 Hour, less than 2.5 Hours
5	Non-Mission Capable	Classified	System Performance Severely Impacted/ Total Loss of Functionality	Greater than 2.5 Hours

The Mission Impact Methodology value for each attack is entered into the Analysis Table.

Analysis Team			
Numerical Mission Impact and Consequence	Attack Cost / Level of Effort	Attack Success Likelihood	Numerica Likelihood
4			
5			

Analysis: Likelihood Assessment

The Cyber Team evaluates attacks using a Likelihood Assessment chart.

How hard is it to do?

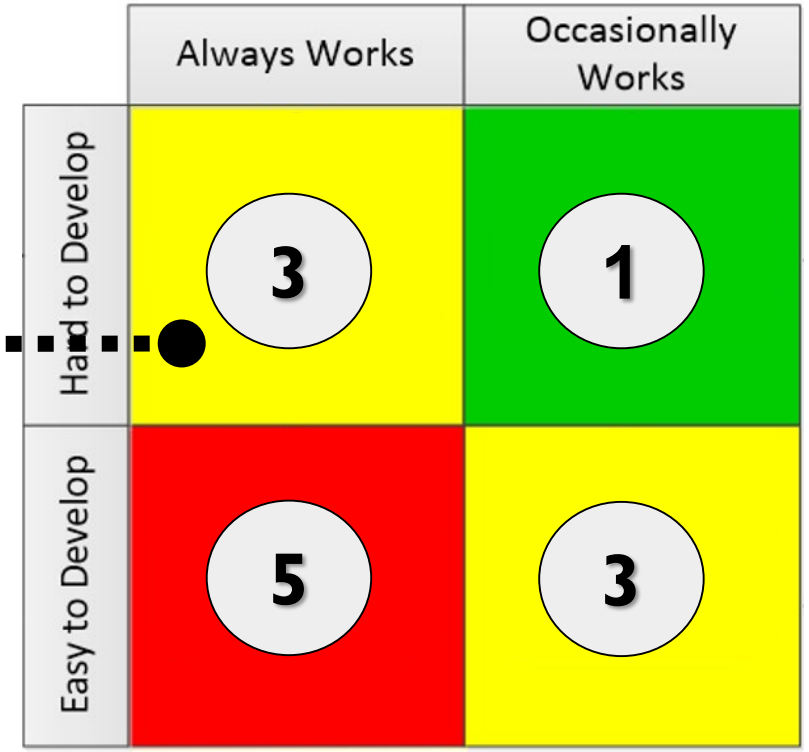
How well does it work?

Attack Cost/ Level of Effort				Attack Success Likelihood: Occasionally works	Attack Success Likelihood: Always works
				Rarely works / Low	Sometimes works / Medium; Always works / High
Nearly anyone can build: Nascent – Limited threat	Low cost to develop	Exists today	Easy to develop	3 — Example: Network DoS	5 — Example: Flash implant delivered via website/email
Criminal level organization can build: Moderate threat	Medium cost to develop	Many can develop			
Nation state organization can build: Advanced threat	High cost to develop	Few can develop	Hard to develop	1 — Example: RF inject of malware into sensor or radio	3 — Example: Supply chain implant in HW or firmware

Analysis: Likelihood Assessment

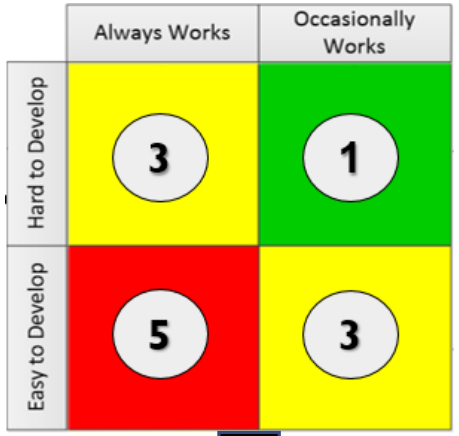
The Likelihood Assessment value for each attack is entered into the Analysis Table.

Analysis Team				
/ Level of Effort	Attack Success Likelihood	Numerical Likelihood	Analysis of numerical Likelihood factoring in access methods. Put new (or unchanged) likelhood value from N.	Final Risk Assessment coordinates
		3		
		4		



Risk Assessment Coordinates

Impact	Mission Impact	Data Loss (MEF)	System Performance (MEF)	Delay (Operational Mission)
1	Fully Mission Capable	No data compromised	System Performance Not Impacted	Less than 5 Minutes
2	Partial to Fully Mission Capable	Public Access Level	System Performance Marginally Impacted	Greater than 5 Minutes and less than 30 Minutes
3	Partially Mission Capable	FOUO	Partial Loss of Functionality	Greater than 30 Minutes and less than 1 Hour
4	Non to Partially Mission Capable	FOUO/New Technology	Major Loss of Functionality	Greater than 1 Hour, less than 2.5 Hours
5	Non-Mission Capable	Classified	System Performance Severely Impacted/ Total Loss of Functionality	Greater than 2.5 Hours

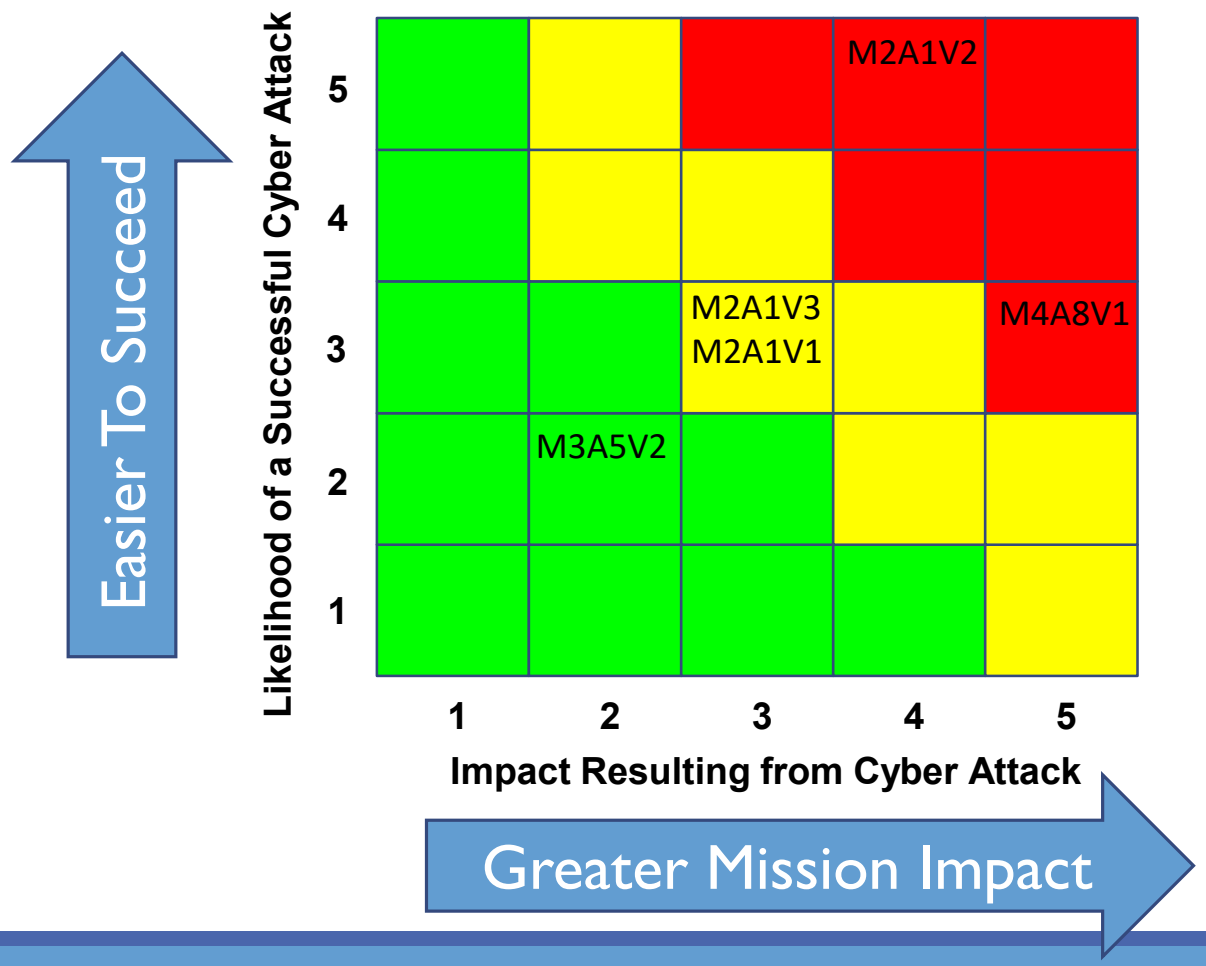


Analysis Team					
Numerical Mission Impact and Consequence	Attack Cost / Level of Effort	Attack Success Likelihood	Numerical Likelihood	Analysis of numerical Likelihood factoring in access methods. Put new (or unchanged) likelihood value from N.	Final Risk Assessment coordinates
4			3		4, 3
5			4		5, 4

Risk Matrix

The CTT risk matrix takes into consideration:

- ✓ The technical feasibility of an attack
- ✓ How well the cyber attack works
- ✓ How hard the cyber attack is to develop
- ✓ The impact to the mission



Helpful Hints

HOW TO MAKE IT SUCCESSFUL

5 Critical Roles

There are 5 critical roles to address to maximize the effectiveness and usefulness of your CTT:

1) CTT Facilitator
2) CTT Lead & Deputy
3) Discussion Facilitator
4) Cyber Team Lead & Deputy
5) CTT Coordinator

"The [cyber] team lead is the most important role in the CTT and choosing the right person is critical to ensure the CTT results are high quality and useful to the Program."

~The Department of Defense Cyber Table Top Guidebook, Version 1.0, Section 3.1.1.3.1

Some of these roles can be filled by the same person (for examples, the CTT Lead's Deputy often does much of the CTT coordination; and the Cyber Team Lead can be the primary Discussion Facilitator)

CTT Facilitator

1) CTT Facilitator

- Suggested for CTT's with inexperienced control teams
- Usually external to the organization
- Extensive experience planning, executing and participating in CTT's
- Guides control team through preparation process, helping to make good decisions early on that will move the CTT towards satisfying the program's objectives
- Provides insights, lessons learned and best practices from other CTTs
- Can help facilitate discussion during CTT execution

CTT Lead & Deputy

2) CTT Lead & Deputy

- Internal to the organization, usually a leader in the community
- Overall authority and responsibility for the CTT
- Understands organizational vision and goals regarding the CTT
- Does not have to be involved in the day to day planning activities (deputy often takes on administrative tasks during preparation phase.)
- Guides discussion during CTT Execution to stay focused on the organization's objectives and within the pre-determined boundaries

Discussion Facilitator

3) Discussion Facilitator

- Facilitates discussion during CTT execution (controls the room)
- Must have the technical knowledge to ensure the correct and complete information has been gathered from participants before moving to the next attack (the cyber-lead can be a good candidate)
- Must have the ability to control the conversation in the room (stop unproductive tangents, make sure the note takers hear everything being said, doesn't cater to the existing hierarchy, doesn't allow one person to dominate the conversation etc…)

Cyber Team Lead & Deputy

4) Cyber Team Lead & Deputy

- DoD Guide book defines this role as the most important to fill with the right person; the cyber team lead should have:
  - Participated in previous CTTs
  - A background in defensive and offensive cybersecurity
  - Effective communication skills
- Without a qualified person to fill this role, the CTT will not provide new or usable information to the program, or (worse) the information provided will not be complete or accurate

CTT Coordinator

5) CTT Coordinator

- The CTT is often an additional duty for those involved, so a successful CTT needs someone (or multiple someones) to keep things moving:
    - schedules the next meeting
    - sends visit request information
    - reserves rooms
    - ensures the room has the correct provisions and supplies
- This role can be filled by an existing member of the control team (such as the control team lead deputy) or a lieutenant in need of more work
- The coordinator ensures the entire process is as organized as possible so the participants can focus solely on the exercise

Note Takers

- A CTT can generate the most stimulating, useful information, but if it's not captured by the Note Takers it won't go beyond the people in the room (and will most likely be forgotten or mis-remembered)
- Experienced Note Takers (or ones familiar with the organization's language, system or participants) are nice, but not necessary
- Invite all Note Takers to the Kickoff Meeting (spins them up on the system, gets them familiar with the key players etc…which facilitates better note taking during the event)
- Invite more Note Takers than you want to have in case some need to back out (DoD Guidebook recommends at least four Note Takers)
- Notes can be hand-written or typed into a computer (computer notes are easier to find information; audio recordings are not easy to analyze)
- Note Takers should not concern themselves with spelling error or typos
- During the exercise, always, always go at the Note Taker's pace (see first bullet point)

Participants

- Ideally all participants would be present throughout the entire CTT
  - It's very important that everyone is present for the system and mission description, threat briefing and rules of engagement (everyone needs to buy into the process for it to work)
  - I recommend against experts popping in and out:
    - It's good to keep everyone's minds focused on the CTT (and not thinking about their inbox)
    - It may seem like an expert only needs to be there when his or her area of expertise is being discussed, but the CTT is dynamic so does not always stay on schedule, and an expert's inputs can be solicited at unexpected times (this is cyber; everything is connected)
  - It's advantageous when the whole community hears what other experts have to say; ideally the whole community walks through the entire process together and collectively buys off on the results (agree which attacks are feasible, which vulnerabilities really do need to be addressed etc…and equally important, which attacks are of less concern, which vulnerabilities are already being addressed and where the community doesn't need to spend as much time and energy)
  - It can be beneficial to cater lunch; the break itself is important, but it can be good to keep everyone together

Participants

- Invite the unofficial leads of the community
  - They can take the principles back to the other members of their community and help implement the results and influence the general attitude towards cybersecurity practices
- Organization leadership needs to emphasize the importance of the CTT
  - Both prior to the event so participants know it's worth their time and effort (especially considering it's usually additional duties), and at the beginning of the exercise to set the atmosphere (it might be helpful to have a community leader welcome everyone to the CTT)
- Program needs to plan/budget for CTT resources
  - Especially if industry contractor support is needed
- Deputies are especially important for critical roles
  - To help carry the workload but also so as not to have a single point of failure

Pre-Exercise Activities

Initial Site Visit

- In the early planning stages anyone not familiar with the system and organization (such as the cyber team) should visit the organization, see where the work is done and look at the system (if possible.) This goes a long way towards getting useful information from the CTT, and also allows those who do not know one another a chance to meet (and start working together.)

Overview Training

- The Overview Training is a TRMC class called "Facilitator Training" that can be tailored for each CTT. Instead of the full class, Edwards opted for a one-day class that gave the community an overview of the CTT and had us run our own mini-CTT to get some exposure to the process.
- This was an especially effective way to engage the community and socialize the idea of the CTT. We invited 25 of the community leaders and people we thought might end up as CTT participants.

Kick Off Meeting

Kick Off Meeting: about a month before the CTT exercise, gather the leaders of the event to review the operational mission and system description

- This gives the control team, operational team and cyber team a chance to coordinate:
  - Make any course adjustments that are necessary prior to the event
  - Exchange any information that will help guide the process (does the cyber team need additional information about the system to identify potential cyber attacks?)
  - Identify what still needs to be addressed prior to the event (is the Mission Impact Methodology developed?)
- Invite the Note Takers to the Kick Off Meeting
  - This gets them familiar with the system and key participants which helps facilitate good notetaking
  - The teams can discuss expectations and explain the process to the note takers

Exercise Activities (Kickoff!)

The CTT exercise can be tailored for each program, but generally starts with the following activities (order varies):

1) Introduction/Welcome from Leadership
2) Administrative Details
3) Threat Briefing
4) Classification Level
5) CTT Overview
6) Rules of Engagement
7) System Definition
8) Operational Mission Description

Threat Briefing

At exercise kickoff, a tailored threat briefing from an intel office can be very effective in making the theoretical concepts much more real and quantifiable.

A threat briefing (~30mins):

- Helps engage the CTT audience
- Begins to focus people's minds on cyber security
- Reduces push-back when the cyber team starts proposing attacks
  - so the CTT spends less time trying to convince the participants that the adversary can execute an attack and more time discussing which attacks are technically feasible

System & Mission Definition

It's critical that everyone participating in the CTT has the same understanding of the operational mission and the system under evaluation:

- The control team is responsible for defining the operational mission (to include boundaries) and selecting the system
- The operational team lead (who is a member of the control team) is responsible for communicating these elements to the CTT participants
- Often this means developing presentations, block diagrams, tables, charts etc…
- And effectively communicating the mission, system and boundaries to the CTT participants at kickoff

Rules of Engagement

The Rules of Engagement (ROE) are important because they facilitate the conversation that is necessary to making the CTT a success. This exercise only works if the people you've invited are willing to share what they know. Here are some examples:

- Non-Disclosure/Non-Attribution/Non-Retribution

  People won't bring up the times they've circumvented cybersecurity if they think they're going to be reprimanded for it.
- Everyone Needs to be Heard

  This can be tricky in the military because we have a well established pre-existing rank structure; but the enlisted personnel or technicians need to be encouraged and able to share. (You also might want to consider this item during participant selection.)
- No Interrupting

  Again, so that everyone can be heard. The event facilitators should enforce this and other ROE's during the exercise.
- No Sidebars

  People are very tempted to have discussions with the people they already know while on breaks; remind everyone before and after a break to wait until the break is over before brainstorming so that everyone (especially the Notetakers) can hear the idea.

Rules of Engagement: Note Takers

It's very important to establish the expectations for interacting with the Note Takers during the event; here are some suggested ROE's to ensure the CTT Note Takers can capture the event accurately:

1) Speak Up (everyone, not just the Note Takers, needs to be able to hear you)

2) Say your name and number before you give your input (every time; this ROE often needs to be reinforced as the event goes on)

3) Hold up your number (if provided- see Name Tag slide)

4) Go at the pace of the Note Takers (if they ask people to slow down, make sure everyone accommodates them)

5) And one more time…no side conversations (everyone's input is valuable and needs to be properly captured)

Classification Level & SCG

- The CTT needs to be at the correct classification level:
  - Unclassified: information might not be useful
  - TS: can be hard to get people you need in the room (some systems have no choice)
  - SECRET: seems to work well for most general systems

  The control team should consider the classification of aggregation of potential vulnerabilities when assigning a classification level to the CTT.
  - Holding a CTT at the SECRET level (even if the system documentation is FOUO or UNCLASSIFIED) protects the potential cybersecurity vulnerabilities while their sensitivity is uncertain

- The Control Team also needs to provide a Security Classification Guide (SCG)
  - The CTT Intelink Website has overarching SCGs available to provide guidance to programs that do not have a SCG that delineates how to handle cybersecurity vulnerabilities

The Room

- Capacity for # of participants and observers
- U-Shapped (or discussion based) table (a classroom or theater setting does not work)
- Classified and/or unclassified projector
- Wall space (to hang diagrams & charts)
- White boards, easels, butcher block or wall sticky pads (& associated writing implements)
- Fans (a lot of people in a small space can get very warm, very quickly)
- Bell (impromptu and half-joking addition, but came in very handy when trying to regroup!)

Event Supplies

- Notebooks (for Notetakers and participants, a variety of sizes depending on preferences)
- Pens (multiple colors)
- Classification Stamp & Necessary Bags
- Stapler
- Tape: both Scotch tape and masking tape or packaging tape (to hang posters)
- Mints (as a curtesy)
- Tissues
- Lotion (mainly for Notetakers)

Name Tags

A very important (but sometimes overlooked) aspect of the CTT dynamic is making it easy for the Note Takers to know who is talking. Note Takers will note the speaker for each comment they document during the event, so it's important that they can easily identify who is talking. Here are a few ways to facilitate this:

1) Traditional lanyard name tags with the name and number
   - This option is good for up close but is not useful if participants are in a larger room
2) Name plate (folded piece of card stock) with name and number
   - Great for participants at a table; does not work for those not around a table
   - Can be used for a subset of CTT participants (perhaps just the team leads/deputies and/or just newcomers to the organization)
3) Number on a stick (that can be held up like at an auction)
   - Can work well for those sitting in chairs but not at a table, but can be difficult for the Note Takers to see

Event Refreshments

- Water
- Coffee & Tea
- Soda (Regular & Diet)
- Fruit Juice (Orange Juice)
- Fruit (Grapes were very popular)
- Donuts/Pastries/Muffins
- Bagels & Cream Cheese
- Tortilla Chips & Salsa
- Nuts
- Candy (M&M's were very popular)
- Paper/Plastic Plates
- Plastics Forks, Spoons & Knives
- Napkins
- Coffee Pot (Tea Kettle) & Coffee
- Coffee Cups, Lids & Sleeves
- Sugar, Sugar Substitutes & Creamer
- Gallon Water Jugs
- Cooler & Ice
- Extension Cords
- Donation Box

We suggested a small donation to help cover costs, which seemed to work very well.

I highly recommend catering lunch; it seems to allow for more coherency between sessions.

Analysis Meetings

There are three analysis meetings that follow the CTT exercise:

1) Analysis Meeting #1
   - Prior to first meeting, the analysis team fills in the analysis table with the information extracted from the exercise notes
   - Typically 4-6 weeks after exercise execution (to allow time to compile notes)
   - Verify inputs to analysis table (did everyone hear the same thing?)
2) Analysis Meeting #2
   - 2-4 weeks after 1st analysis meeting
   - Fill in remaining information (based on Mission Impact Methodology and Likelihood Assessment rubrics)
3) Analysis Meeting #3
   - 2-4 weeks after 2nd analysis meeting
   - Identify attacks to present to leadership
   - Develop leadership and community briefs

A subset of the Control Team and Cyber Team attend these meetings.