White Sands Missile Range

Lessons Learned and Recommendations for Conducting a Cyber Table Top in T&E

Tristan C. Gilbert - CISSP

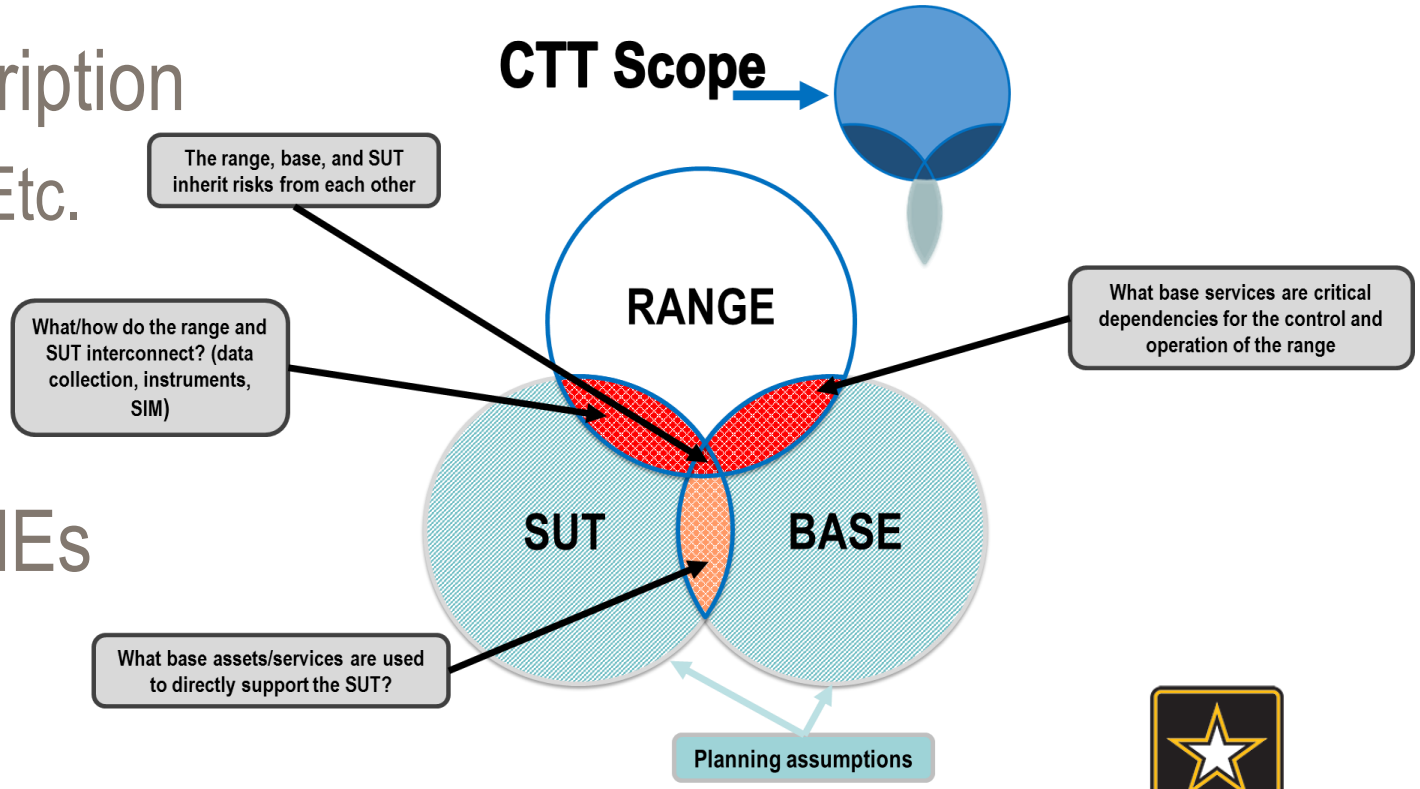
07 March 2018

CTT Purpose

- Low Tech, Low Cost, Intellectually intensive exercise
- Provide actionable information on potential vulnerabilities
  - —Typically does not include threat info
- Accomplished via a likelihood of success vs impact risk scoring system

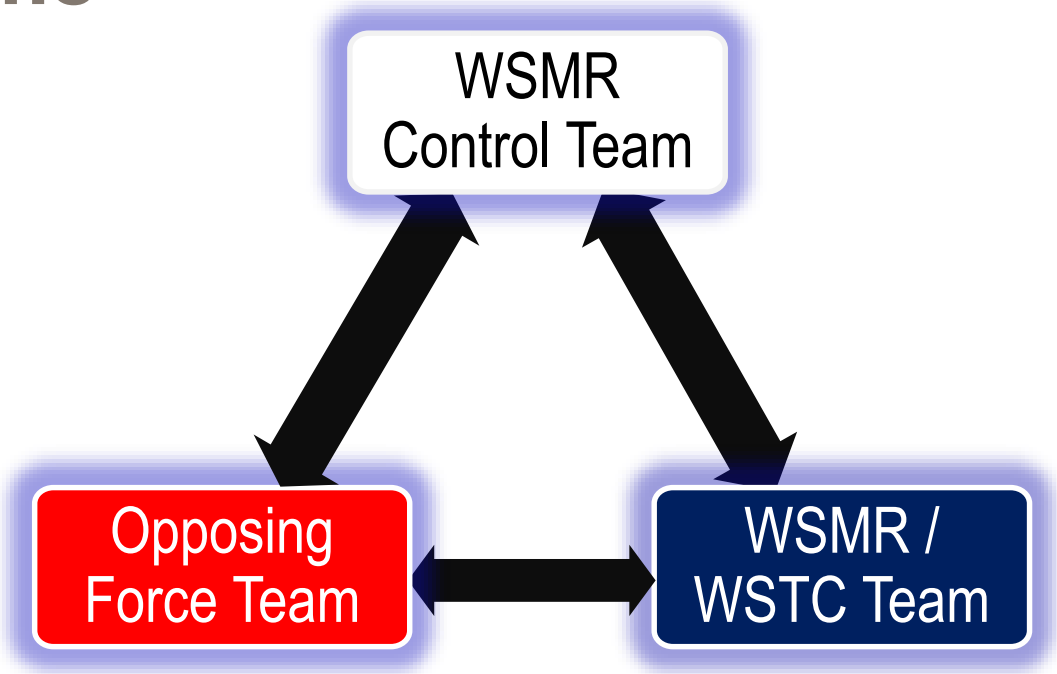
Approach to CTT Exercise

- Identify Critical Cyber Domain
- Scoping
- Representative Threat Description
  - —Capabilities, Access, Reach, Etc.
- Rules of Engagement
  - —Classification Considerations
- Identify and Engage Key SMEs
  - —Non-attribution critical



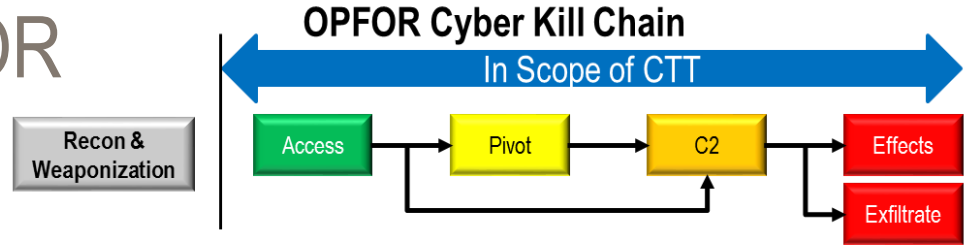
CTT Teams

- White/Control Team
  - Provides Leadership and Management for the exercise
- Blue/Operational Team
  - Provides SME support for operation of systems
  - Provides information on countermeasures for suggested attacks
  - Provides impact assessments on suggested attacks
- Red/Opposing Team
  - Create cyber missions, attacks, and variants



Red Team Approach

- Based on Critical Cyber Domain Develop Mission Set
- Access, Destroy, Disrupt, Degrade, Collect, Exfiltrate
- Ensure participation of experienced OPFOR
  - —Knowledge of the "Art of the possible"
  - —This can be key training point for resident cyber and non-cyber workforce
- Develop Attacks and Variants
  - —Be specific, requires conceptual (high level) overview of actual process, not demonstrated



Recon and Weaponization: Collect data on systems and developing cyber weapons
Access: Inserting a cyber weapon onto a computing system within the platform
Pivot: moving cyber weapons between computing systems within the platform
Command and Control (C2): Establishing bidirectional communication with a cyber weapon operating within the platform
Effects: Using a cyber weapon to conduct availability or integrity attacks against the platform
Exfiltrate: Using a cyber weapon to conduct confidentiality attacks against the platform

Red Team Attack Considerations

- Access/Exfiltrate
  - Supply Chain injection/manipulation
  - Equipment Maintenance/Upgrades – outside organization
  - Consider external network connections, and how information gets on and off the network
  - Wireless – consider non 802.11 variants
- Destroy, Disrupt, Delay, Degrade
  - Common/Well known security vulnerabilities
  - Consider Internet of Things (IoT), Remote Access and Management
  - Single Points of Failure

Cyber Threat Risk Matrix (Notional)

LIKELIHOOD (Y)						
	5	Very Low	Low	Moderate	High	Very High
	4	Very Low	M2A1V3	Moderate	High	M2A1V2
	3	Very Low	Low	Moderate	Moderate	High
	2	Very Low	Low	Low	Low	Moderate
	1	Very Low	M2A1V1	Very Low	Low	Low
		1	2	3	4	5
		IMPACT (X)				

How to read risks on the cube:

- Successful execution of the second variant of attack one for OPFOR mission 2 would leave system non-mission capable
- This attack is highly likely to work based on the assumptions that the adversary
  - Gains access and the required privileges on the network to execute the attack
  - Launches a successful effect against system under test

M: OPFOR Mission
A: Attack
V: Variant

Likelihood is NOT a assessment of the adversary's intent to conduct the specific attack; NOR the probability the SUT will be exposed to the attack

Action Priority Approach

	Risk Level Value	Risk Level
	5	Very High
	4	High
	3	Moderate
	2	Low
	1	Very Low

For each attack:

- Risk level is assigned a value
- Recommended Action is assigned a value based on required next step
- Product of Risk Level and Recommendation Rating provides an Action Rating

	Recommendation Rating	Recommendation
	4	Further Analysis
	3	Test
	2	Mitigate
	1	Accept Risk

Action Ratings suggest priority for follow on CTT phases

- An attack rated as a 15 Action Rating should be considered for further test before an attack rated as a 6 Action Rating
- Action Ratings are objective mathematical suggestions, but all data should be considered when deciding courses of action against CTT findings

Benefits/Lessons Learned

- Paradigm Shift – Consider Cyber in acquisition, deployment, and ops
  — Technical Difficulty or Cyber Attack
- Insight for non-cyber focused workforce (Cyber Domain Awareness)
- Training for blue/red/white teams (incl. SMEs) on things to look for
- Need for integration with intel piece
- Data Aggregation/Big Picture Insight
- Assessment and Justification of Cyber workforce staffing requirements
- Detection, Prevention, Attribution capabilities/gaps
- Insider Threat Working Group
- Top down support for Cyber Efforts Required
- Cyber is often Bypassed for Convenience