ITEA 6th Cybersecurity Workshop

Identifying Requirements and Vulnerabilities for Cybersecurity: Or How I Learned to Stop Worrying and Love the Six-Phase Cybersecurity T&E Process

Michael G. Lilienthal, Ph.D., CTEP

Electronic Warfare Associates

March 2018

Keep this in mind as we design, develop, test, and field systems

“Pay attention to your enemies, for they are the first to discover your mistakes”

- **Antisthenes**

Problem: Cybersecurity Requirements

SPAWAR Chairs the Information Technology/Information Assurance Technical Authority Board

Navy Information Warfare Industry Day 15 June 2017:

Question to RADM Becker Commander, SPAWAR: Can you give an example of RFP/CDRL language that comes closest to describing what the Navy wants a cyber resilient system to look like?

Response: a worthwhile question and we are working to provide a thoughtful answer to it. My intent is to post a response to a public-facing page for all to benefit.

Problem: Cybersecurity Requirements

WEST 2018 Conference 6-8 Feb 2018 San Diego

Question to RADM Becker: Do you have an example of RFP/CDRL language that comes closest to describing what the Navy wants a cyber resilient system to look like?

Response: No. N2N6 is developing guidance

Chief of Naval ***Operations for Information Warfare (DCNO N2N6)***

In lieu of hard requirements you could:

A) Wait for definitive guidance

B) Make sure the System Under Test (SUT) is in compliance with standards (e.g. NIST)

C) Identify & assess the highest risk cyber threats prioritized by their effects to the SUT's mission with only vague guidance on the adversary capabilities

Recommend B and C

Two Separate Policies to address Cybersecurity

AT&L Risk Management Framework (RMF)

- Categorize System
- Select Controls
- Implement Controls
- Assess Controls
- Authorize System
- Monitor Controls

DOT&E Cybersecurity T&E Process

- Understand Cybersecurity Requirements
- Characterize Cyber Attack Surface
- Cooperative Vulnerability Identification
- Adversarial Cybersecurity DT&E
- Cooperative Vulnerability & Penetration Assessment
- Adversarial Assessment

AT&L RMF – Open Loop

DOT&E – Closed Loop

Why they were developed

AT&L Risk Management Framework (RMF)

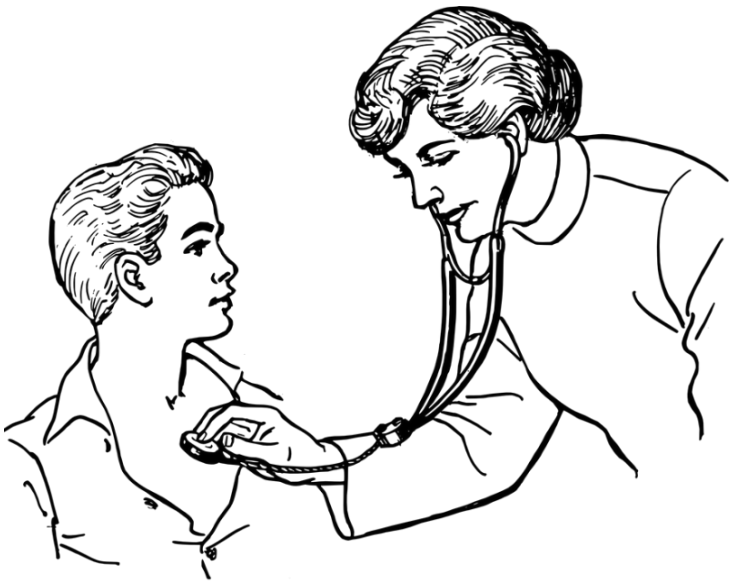
- Secure information systems
- Assess the risk of threats to Confidentiality, Integrity, & Availability (CIA)
- Make design and security control decisions to ensure system operates securely in a high threat environment
- Proactive compliance driven to get the authority to operate (ATO) certification

DOT&E Cybersecurity T&E Process

- Mitigate surprise in systems during Operational Test (OT)
- Many systems that enter OT were not resilient to basic cyber threats
- No time in OT schedule to address the discovered problems
- Increase discovery earlier in the acquisition process

AT&L Risk Management Framework (RMF) Process

- Get Authority to Operate (ATO) certification



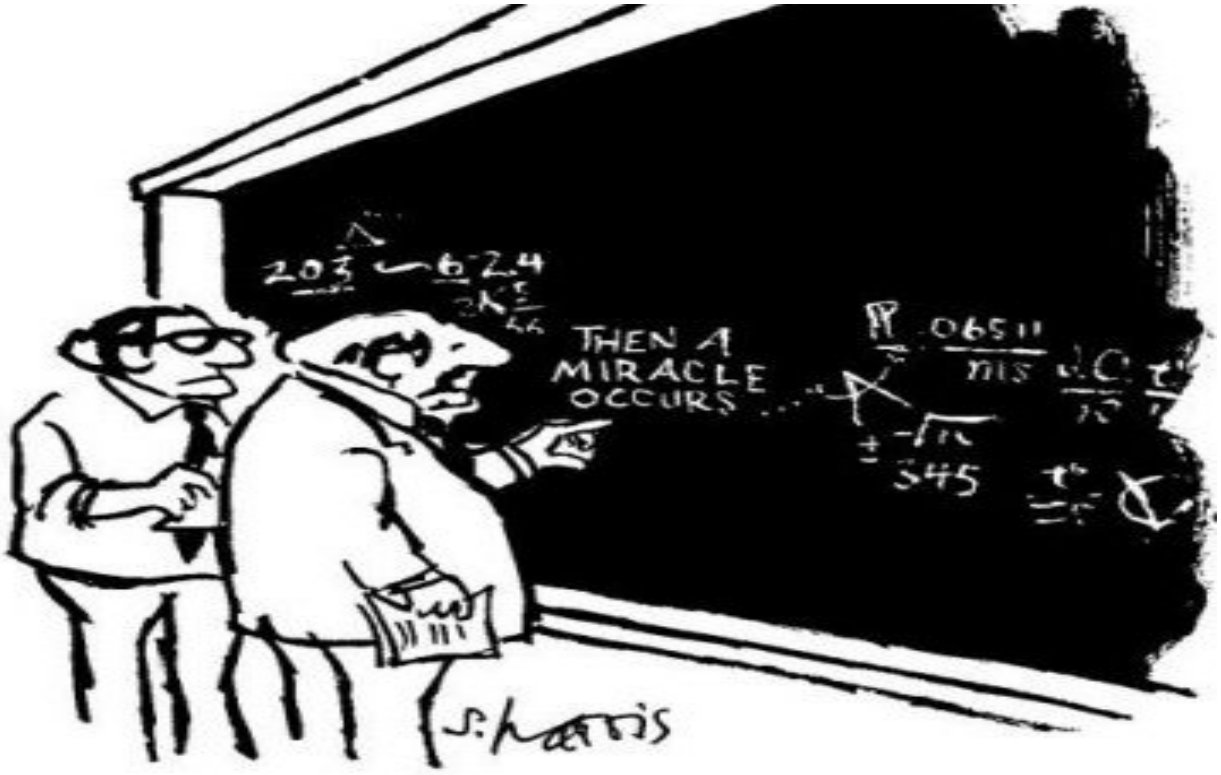
Is my blood work normal?

DOT&E Cybersecurity T&E Process

- Assess how the mission can be degraded or disrupted by exploiting system vulnerabilities

How many ways can I break in and kill your mission?

How do I get started?

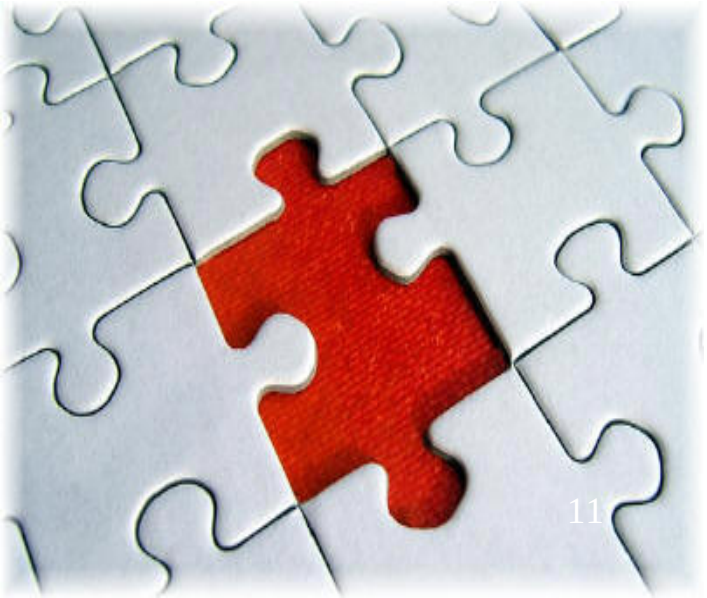


"I THINK YOU SHOULD BE MORE EXPLICIT HERE IN STEP TWO."

What we* did: Leveraged a tool used by the Navy War College since 1886

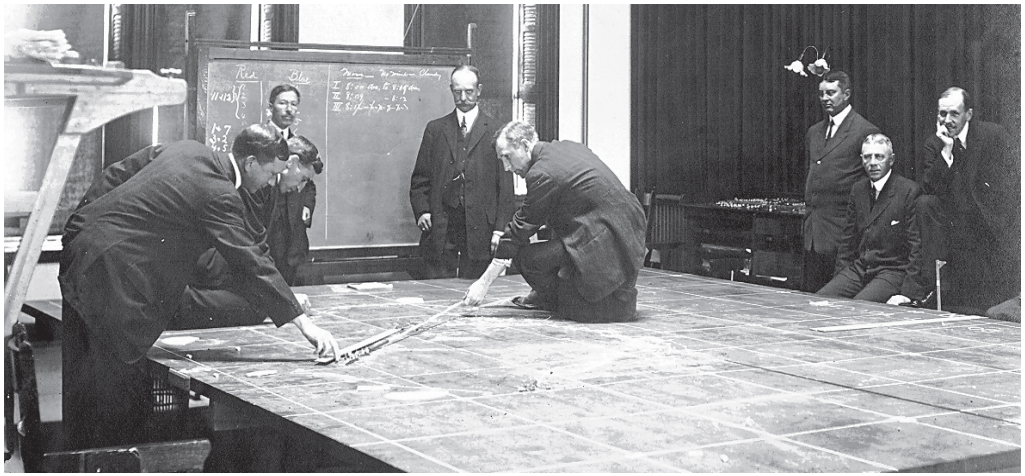
"Wargaming is a tool for exploring decision making possibilities in an environment with incomplete and imperfect information"

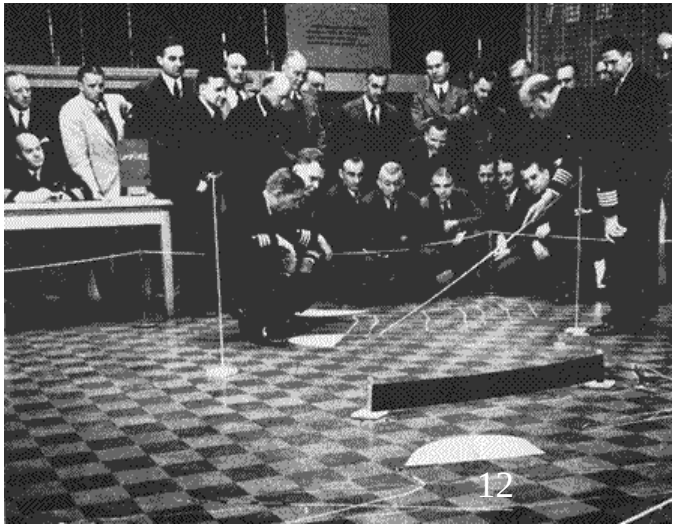
(Herman, Frost, & Kruz, 2009)



* ***NAVAIR P-8 Inc 3, National Cyber Range, & Electronic Warfare Associates***

Naval War College (Interwar period)



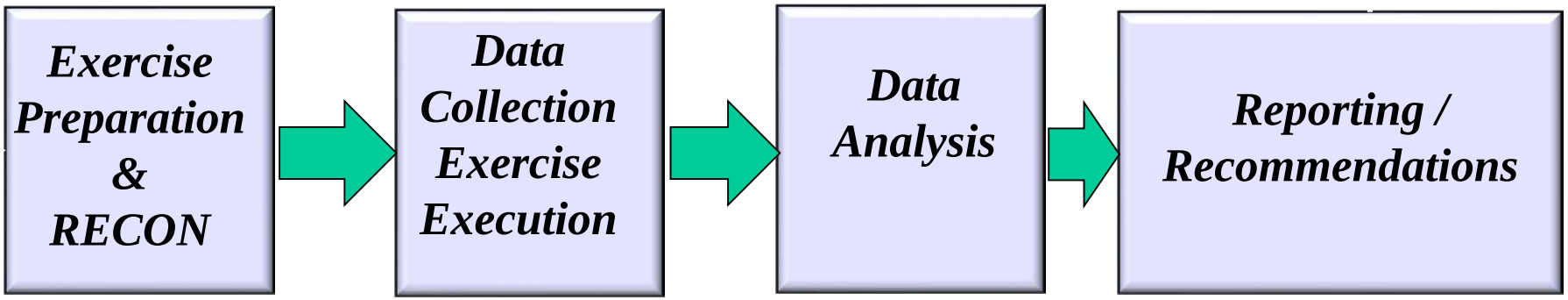


Key Objectives of the wargaming approach for T&E

- Focus on understanding the cyber threat
- Use mission success as the metric
- Design for team collaboration and education
- Explain cyber in the operators' language
- Apply disciplined analytical rigor
- Make the results manageable and actionable

Process had to be easy to execute, low cost, and effective

Result: Cyber Table Top (CTT) Process*



* *NAVAIRSYSOM has a Guidebook for the CTT*

Data Collection Flow: Focus on Threat Mission

Operational Team: Mission Planning

OPFOR Team: Review Reconnaissance Data & attack surface

Develop Mission Plan

Operational Team: Brief mission execution

OPFOR Team: Brief Cyber Kill Chain opportunities

Assess potential attack surfaces

Combined Team: OPFOR Mission Order #1 - #N

Lessons Learned

What Did Programs Gain from using the CTT?

- Justified resource requests and timelines
- Drove improvements
- Identified priorities
- Made it a manageable and affordable problem
- Educated

What Did Programs Gain from using the CTT?

- Justified resource requests and timelines for Cyber T&E through early threat and vulnerability assessment
- Drove improvements through the understanding of the cyber threats in the language of the operational mission
- Identified priorities within the attack surfaces to be countered
- Made it a manageable and affordable problem by binning threats into 3 buckets: Accept, Analyze, Must Test
- Educated cybersecurity personnel by warfighters

What Programs Learned

- Access to the network should be assumed possible
- Goal is preserving Operational mission
- Missions cut across platforms and program offices

What Programs Learned

- Access to the network should be assumed possible albeit hard even in a robustly protected system
- Goal is preserving Operational mission and disrupting OPFOR's kill chain; NOT about a checklist of controls
- Mission focus makes the new threat understandable in the language of the warfighter
- Missions cut across platforms and program offices – system resiliency and survivability are fostering increased cooperation across program office stovepipes

What Testers (T&E) Learned

- Every communication path represents a risk to security but budgets cannot sustain testing every one
- Compliance is necessary but not sufficient
- Cannot keep the hackers out of our networks all the time
- Cyber red teams have little time to participate before OT
- Testing components and subsystems help discover and understand threats early (in EMD)
- Learn the most by doing (along side a skilled red and cyber T&E team member)

What System Engineers (SE) Learned

- Strong bias towards access is NOT possible is no longer correct
- Checklist and compliance assessments do little to ensure system is resilient to cyber threats
- IT implementers do not have mission awareness or experience
- There are opportunities for effective cyber T&E to drive SE processes and RMF and CS processes
- Patterns of common pathways provide useful information to system engineers
- Waiting to conduct effective cyber T&E till after EMD is a bad strategy
- Design changes could disrupt the Cyber Kill Chain if used early
- RFP language needs to clearly state what the selection value and requirements are for cyber resiliency (and emphasize it is more than “do RMF”)

Final Thoughts

Programs that used the CTT process

- **Navy**
  - NAVAIR manned aircraft (P-8A, CH-53)
  - UNMANNED (UCLASS, Triton)
  - CVN-78 Machinery Control, EMALS / AAG, ALRE (Carrier Systems)
  - TACMOBILE (Logistics System)
  - DCGS-N (Intel)
- **Army**
  - JEMN (Radio / comms)
  - White Sands Missile Range
  - Mission Command (Battle Command)
  - DSGS-A (Intel, planned)
- **Air Force**
  - GPS OCX
  - Eglin AFGB
  - Patrick AFB Eastern Test Range
  - Edwards AFB (planned)s
- **Many others conducted:**
  - Some use exact process
  - Some use tailored process
  - DT&E support some
  - Some programs / agencies do their own or other process

Feedback on July 2016 CTT

"… the event was a "game changer", in that it not only helped identify vulnerabilities, but it tied them to mission risk and also helped with the culture change necessary to get our entire workforce behind this important topic. Getting our engineers, fleet, and program offices to understand exactly what a potential adversary could do to a ship's ability to safely and efficiently launch and recover aircraft was worth it alone. We will be using the results from this event to drive POM requests, recommend technical fixes, plan further analysis/testing, as well as change some of our internal processes."

Ms. Kathleen P. Donnelly SES
NAVAIR 4.8
Director, SE & ALRE Engineering

Points of Contact

- NAVAIRSYSCOM CTT Handbook –
  - Paola Pringle paola.pringle@navy.mil
- Electronic Warfare Associates
  - Michael Lilienthal Mlilienhal@ewa.com 571-238-4532
- Lockheed Martin NCR & CTT Team
  - Patrick Lardieri Patrick.j.lardieri@lmco.com

Questions?