412th Test Wing

412TW

War-Winning Capabilities … On Time, On Cost

U.S. AIR FORCE

The Merge of Electronic Warfare and Cybersecurity Test

8 May 2018

Lt Col Jose R. Gutierrez

Outline

- Motivation
- Introduction
- Cyber as an operational environment
- Electronic Warfare (EW) Platform Test
- The Merge
- Weapon System Cybersecurity Test Approach
- A Fictional Case
- Closing Remarks

But first...

- Caveat #1: I am NOT a cyber tester nor a cyber expert
- Caveat #2: This brief is NOT about how to test cybersecurity

Motivation, from Dr. Kendall

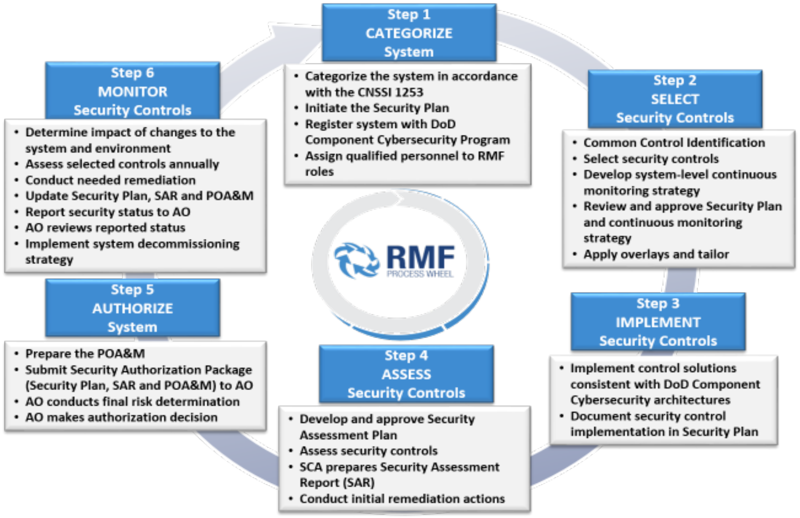
“**Cyber testing and the ability to achieve a “Survivable” rating in an official operational test environment continues to be nearly impossible for a Program of Record (POR) to achieve.** Test criteria are not well defined and, even if requirements are met, the standards and scope is “independently” determined by the OTA or DOT&E for success. The threat portrayal often exceeds the capabilities of a Blue Force Team (i.e., nation-state threat going against a brigade-level formation), focuses more on “insider” threat of unreasonable proportions, and minimizes the importance of “defense in depth” approach. **Recommend better definition for standard cyber rules of engagement at operational test**, the allowance for external cyber protection teams, **and that test reports focus on the program under test** (not the overall “network”)”

Kendall, Frank, *Kendall DAU Magazine*, July-August 2016

Intro

- Initial focus of cyber test is centered around IT systems, networks and IT systems in platforms

- Risk Management Framework is a systematic way to test and certify IT and PIT systems for operations. It is mandated by DoDI 8510.01



Step 1
CATEGORIZE
System

- Categorize the system in accordance with the CNSSI 1253
- Initiate the Security Plan
- Register system with DoD Component Cybersecurity Program
- Assign qualified personnel to RMF roles

Step 2
SELECT
Security Controls

- Common Control Identification
- Select security controls
- Develop system-level continuous monitoring strategy
- Review and approve Security Plan and continuous monitoring strategy
- Apply overlays and tailor

Step 3
IMPLEMENT
Security Controls

- Implement control solutions consistent with DoD Component Cybersecurity architectures
- Document security control implementation in Security Plan

Step 4
ASSESS
Security Controls

- Develop and approve Security Assessment Plan
- Assess security controls
- SCA prepares Security Assessment Report (SAR)
- Conduct initial remediation actions

Step 5
AUTHORIZE
System

- Prepare the POA&M
- Submit Security Authorization Package (Security Plan, SAR and POA&M) to AO
- AO conducts final risk determination
- AO makes authorization decision

Step 6
MONITOR
Security Controls

- Determine impact of changes to the system and environment
- Assess selected controls annually
- Conduct needed remediation
- Update Security Plan, SAR and POA&M
- Report security status to AO
- AO reviews reported status
- Implement system decommissioning strategy

Intro

- IT in Weapon Systems?
- Platform IT (PIT)
  - Subject to Assessment and Authorization (A&A)

Intro

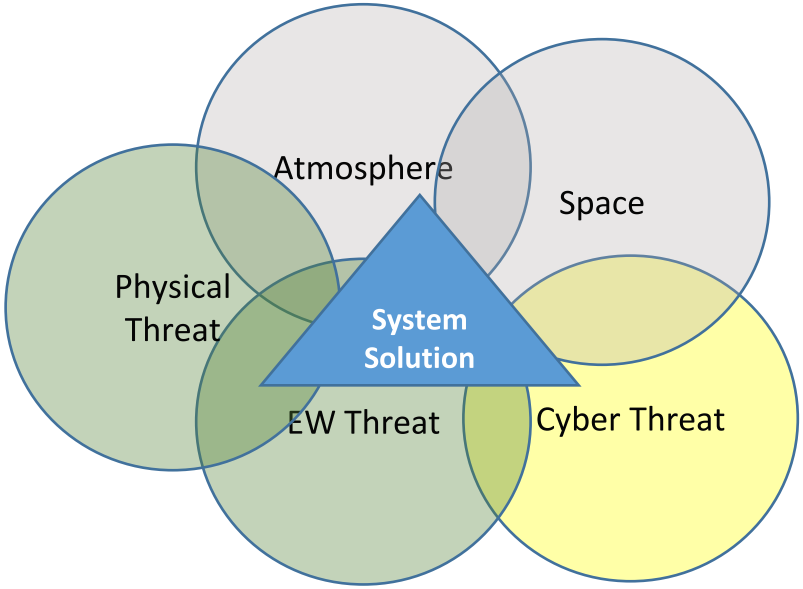
- So there is a process to address cybersecurity of IT and PIT systems, but what does it mean to an operator in the middle of a mission?

- How about: The ability of the weapon system to conduct operations in a cyber-contested environment? Who tests that?

- We’ll skip the IT centric test, policies, and processes and ASSUME, that the IT configuration in the PIT system is authorized for operation.

Cyber as an operational environment

Physical Environment



Operational Environment

Cyber is analogous to every other operational and physical environment

The Merge

Air Force Space Command Commander,
General John Hyten:

“In cyberspace, we provide pathways for information, we deny adversaries information. It’s the same [EW] mission… that we do in different domains.”

[Amber Corrin, C4ISRNET, “Cyber and EW: It’s all about effects, not omissions”]

The Merge

- A platform EW system must be able to provide mission assurance by protecting and ensuring the functionality of its on-board systems when encountering electromagnetic attacks.

- A platform cybersecurity system must be able to provide mission assurance by protecting and ensuring the functionality of its on-board systems when encountering cyber attacks.

- A platform EW system must be able to provide mission assurance by protecting and ensuring the functionality of its on-board systems when encountering cyber attacks.

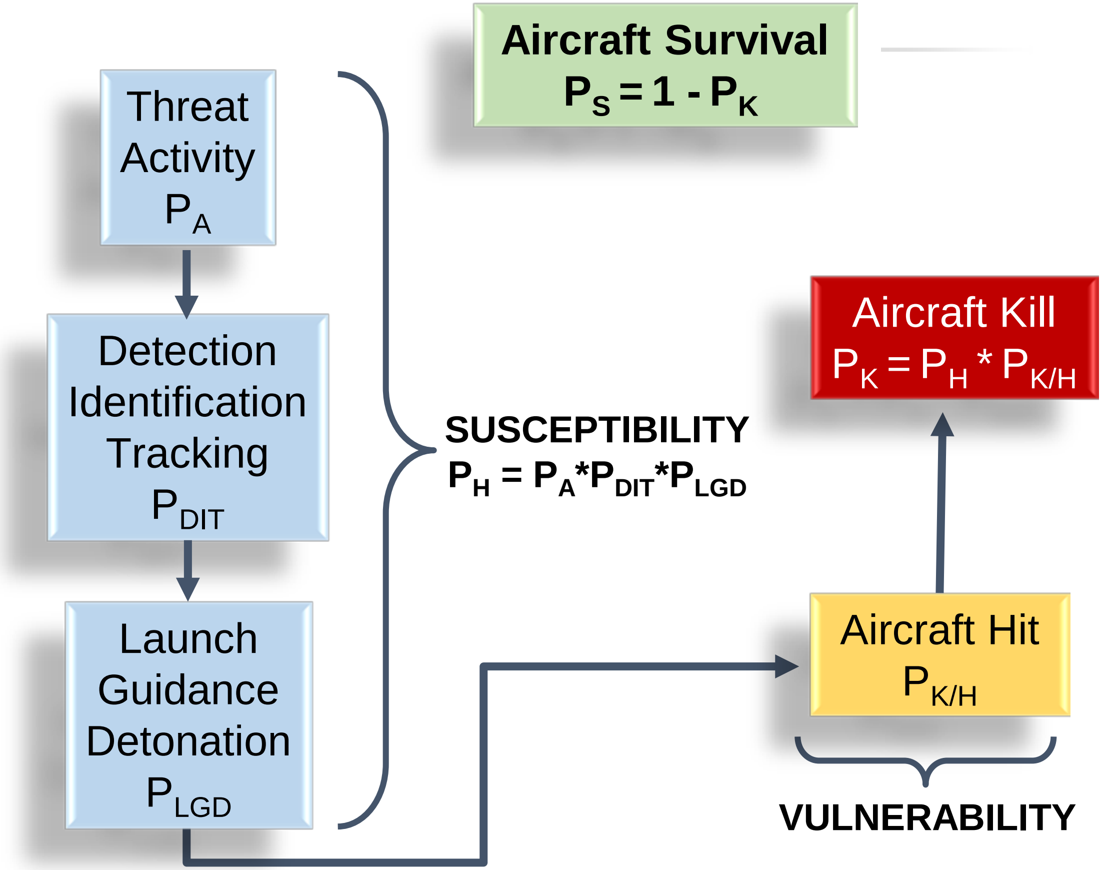
IT’S ALL ABOUT MISSION IMPACT

EW Survivability

Survivability: The capability to avoid and withstand a man-made hostile environment

Susceptibility: The inability to avoid threats

Vulnerability: The inability to withstand threats



Aircraft Survival

$P_S = 1 - P_K$

Threat Activity

P_A

Detection Identification Tracking

P_{DIT}

Launch Guidance Detonation

P_{LGD}

SUSCEPTIBILITY

$P_H = P_A * P_{DIT} * P_{LGD}$

Aircraft Kill

$P_K = P_H * P_{K/H}$

Aircraft Hit

$P_{K/H}$

VULNERABILITY

EW helps decrease susceptibility (P_H)

Cyber Survivability

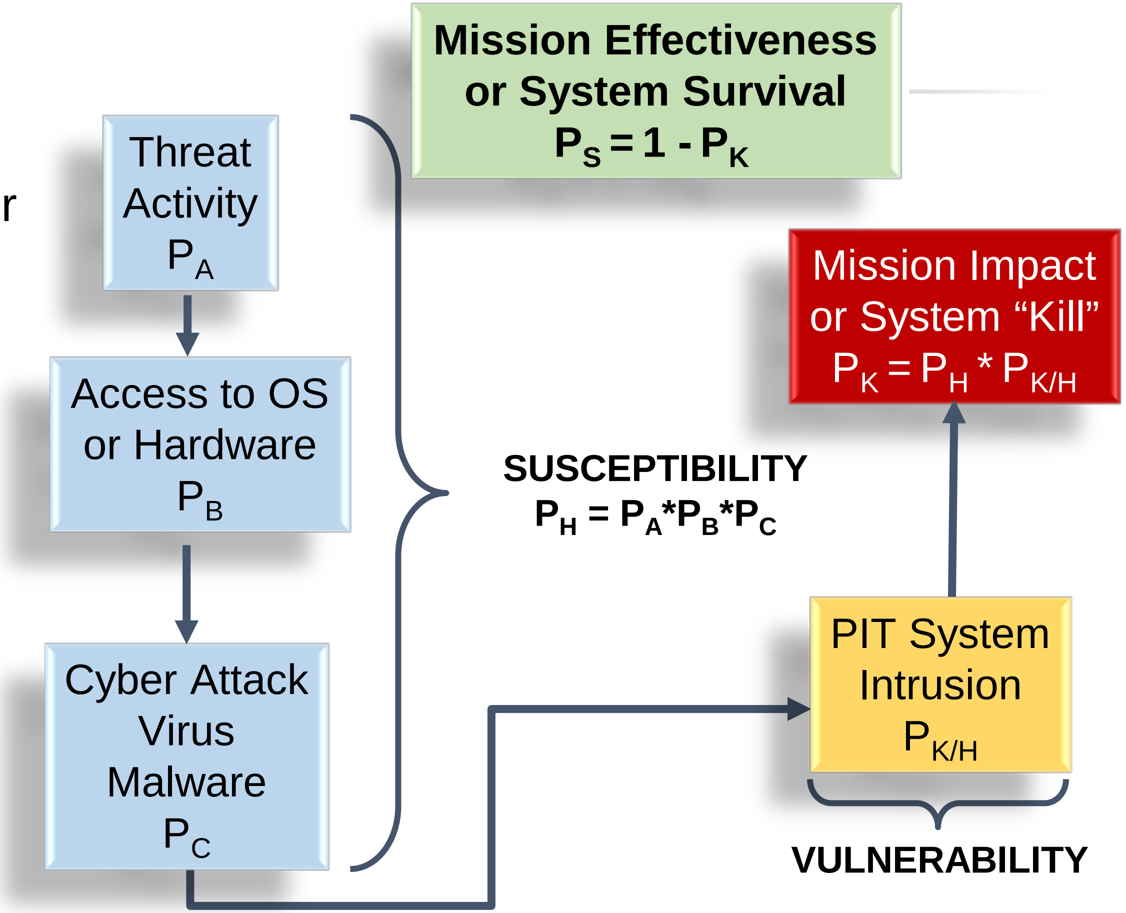
Added Mission Effectiveness or mission impact because of other possible effects

Same model applies,
it is still effects-based!

$$P_K = P_H * P_{K|H}$$

$$P_H = \prod_{i=1}^{N} P_i$$

(you have to have some MATH!!)


Mission Effectiveness or System Survival $P_S = 1 - P_K$
Threat Activity P_A
Access to OS or Hardware P_B
Cyber Attack Virus Malware P_C
Mission Impact or System "Kill" $P_K = P_H * P_{K/H}$
SUSCEPTIBILITY $P_H = P_A * P_B * P_C$
PIT System Intrusion $P_{K/H}$
VULNERABILITY

Cybersecurity helps decrease susceptibility (P_H)

Other Analogies

EW Domain	Cyber Domain
Radar Warning Receiver	*Intrusion Detection System*
Track Quality	*Software Integrity*
Detection and Identification	*Access to operating systems, or hardware*
False Targets, false position/velocity data	*Data Corruption, Hacking, loss of system control*
Threat Activity & Means	*Threat Activity & Means*

Cyber Threats

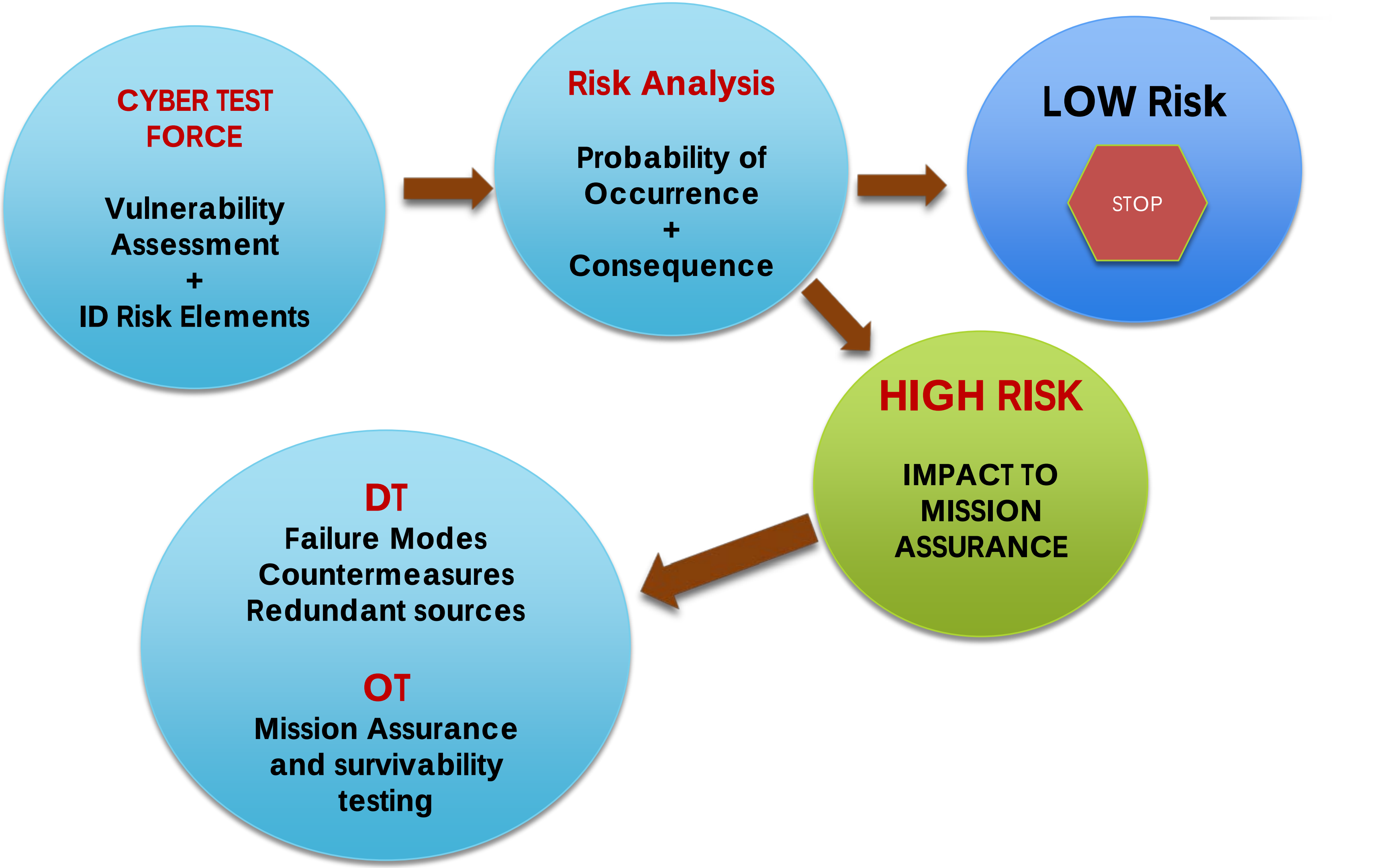
Think of EVERY software virus, every piece of malware, every intrusion tactic, known and unknown in the world.

Each one poses some level of threat to our weapons systems.

TEST THEM ALL?

100% cyber-proof system is impossible, but we can design test around the most “likely scenarios”

So how do we approach this?



CYBER TEST FORCE

Vulnerability Assessment
+
ID Risk Elements

Risk Analysis

Probability of Occurrence
+
Consequence

LOW Risk

STOP

HIGH RISK

IMPACT TO MISSION ASSURANCE

DT

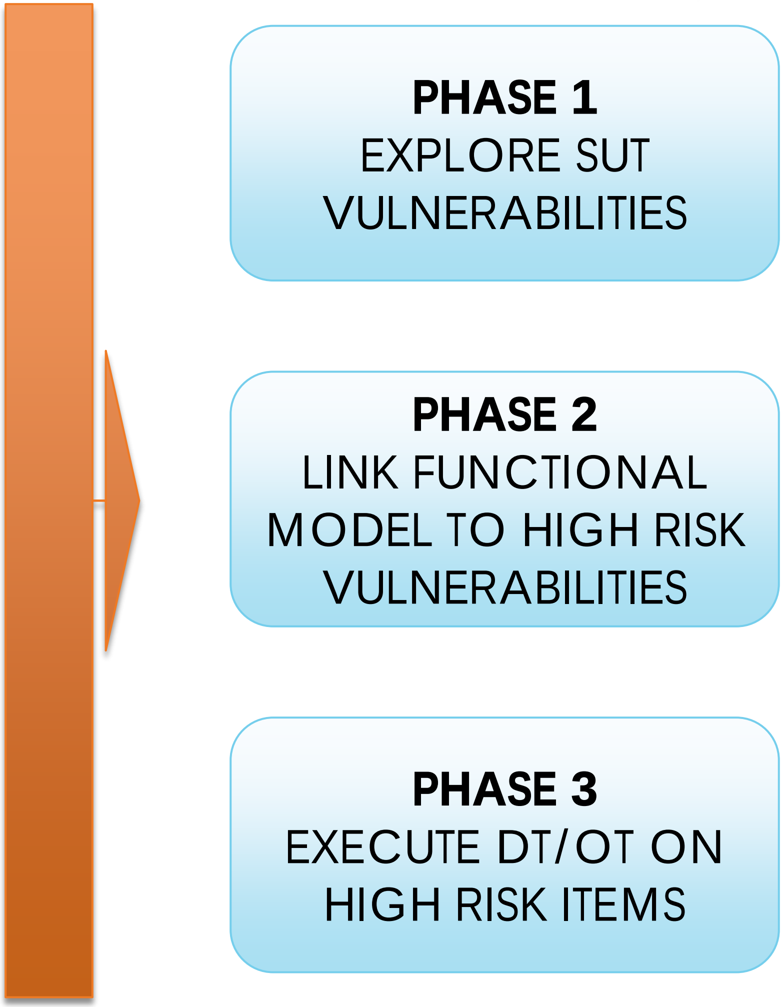
Failure Modes
Countermeasures
Redundant sources

OT

Mission Assurance and survivability testing

TO DO LIST

- Thorough SYSTEM analysis breaking down subsystems, data buses, information, flow, internal and external connections, etc.
- Perform a thorough functional analysis of the SUT
- **Find the critical links between function and system architecture**
- Define mission operational requirements
- Identify current and future threats to mission accomplishments
- TEST SUT operations in presence of threats
- Develop tactics, procedures, or counter systems based on results



PHASE 1
EXPLORE SUT VULNERABILITIES

PHASE 2
LINK FUNCTIONAL MODEL TO HIGH RISK VULNERABILITIES

PHASE 3
EXECUTE DT/OT ON HIGH RISK ITEMS

A fictional case study

Joint Air-Ground Dual Attack Penetrator (JAGDAP)

- Cyber-resilience in early design
- Uses OMG RF link integrated with platform's GPS/INS for navigation

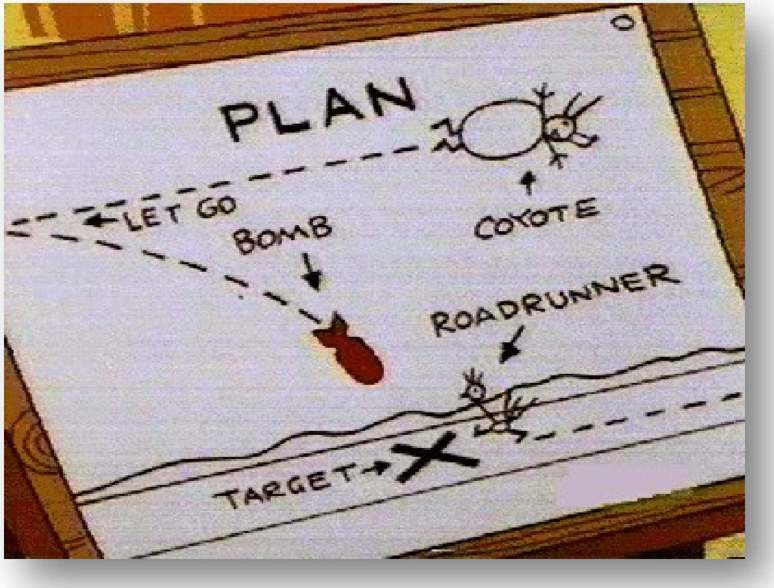
B-55 Coyote

Cyber-resilience in early design

Omni Munition Ground (OMG) Network

- Controlled by deployable mobile stations
- Provides up-to date target coordinates

JAGDAP OV-1



A fictional case study

PHASE 1

PIT System cleared for operation

Cyber, intelligence, contractor team explore vulnerabilities (platform + weapon)

One Vulnerability not planned for:

- OMG Network can be hacked through ground station
- Hacker could change data and control messages

A fictional case study

PHASE 2

OMG Network attack could bypass the platform tracking correlator and inject false targeting information into JAGDAP

OPERATOR can lose total weapon control

Severe Mission Impact, could be deadly to blue ground forces and allies

Threat Susceptibility Assessment

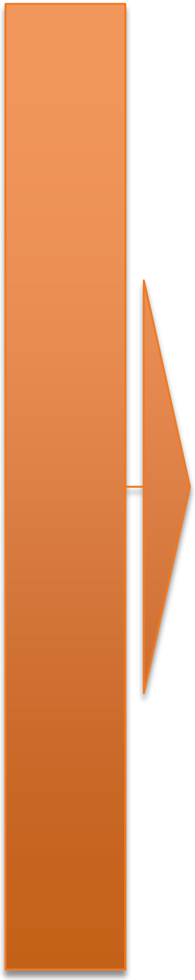
Susceptibility	P_i
Threat exists in area of operation	1.0
Access to OMG ground networks	0.8
Identification of weapon system	0.9
Discovery of vulnerability	1.0
Adversary timely reaction to discovery	0.9
Successful intrusion	0.7
Successful effect given intrusion	1.0
Susceptibility P_H	**0.45**

A fictional case study

PHASE 3

DT/OT Team assumes worst case and evaluates mission effectiveness:

- Onboard fusion engine actually protects other platform’s EW systems – no impact found
- No current EW or Cyber countermeasures will prevent loss of JAGDAP control
- Survivability of platform assured – out of weapon range
- Mission effectiveness severely reduced



RECOMMENDED TACTICS

DISABLE OMG CONNECTIONS

USE STANDOFF TARGETING SUPPORT

PROTECT GROUND UNITS

WRAPPING IT UP

- It’s all about effects; high systems engineering workload upfront necessary
- To EW test, cyber is just another threat
- Risk analysis and susceptibility assessment help manage the infinite amount of cyber attack possibilities
- As threats evolve, DT/OT must reassess

QUESTIONS?