INFORMATION ASSURANCE TESTING:

JAMMING IS NO LONGER ENOUGH

EPG

Presented by Colonel Hugo Keyner
Commander, Electronic Proving Ground
Fort Huachuca, AZ

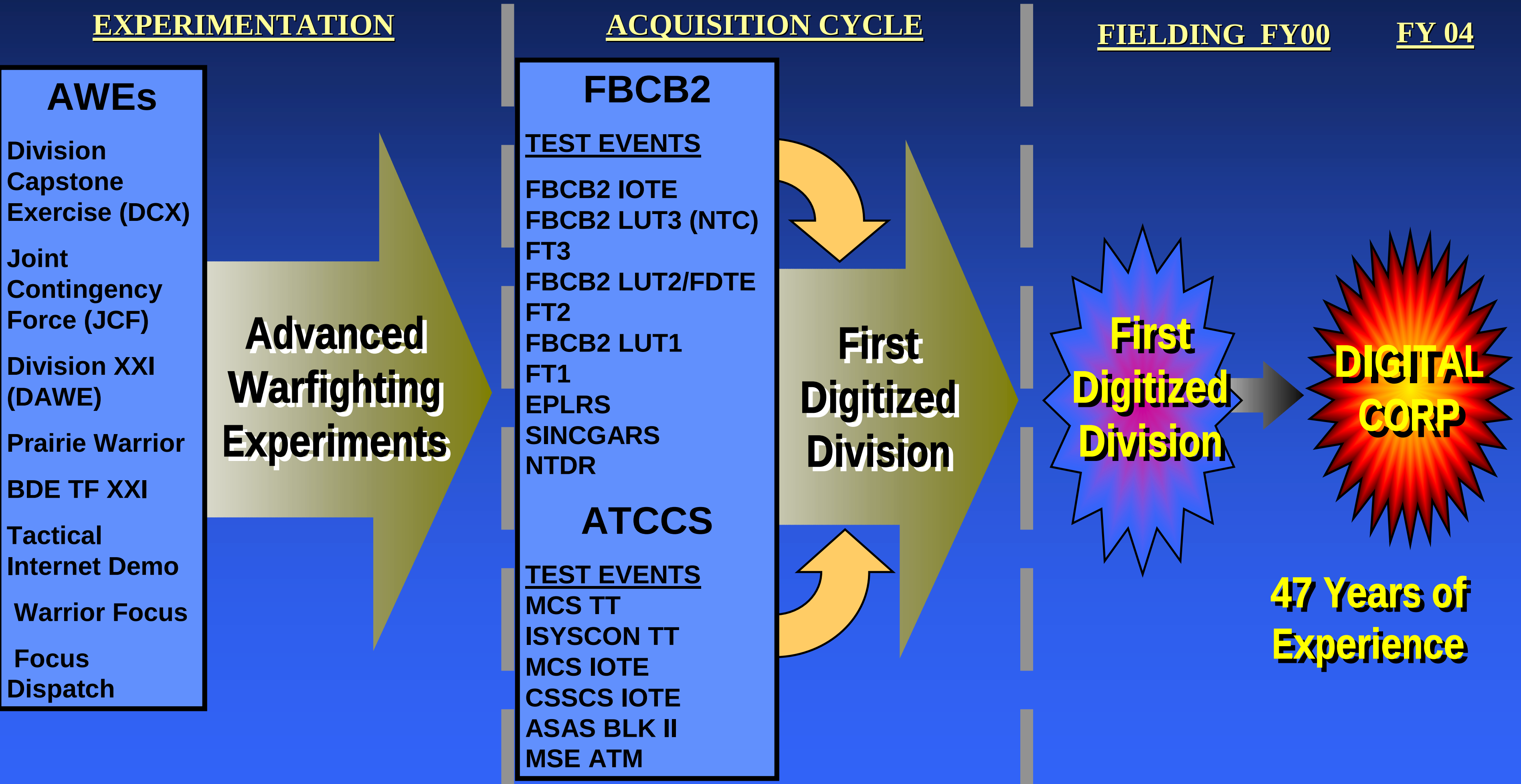
26 April 2001

Agenda

- EPG’s role in Army C4I Testing
- Our approach to testing IA
- Challenges in IA Testing
- Thoughts on how to improve IA Testing

An approach of IA testing for Tactical C4I Systems

EPG'S ROLE – Development Testing for Army C4I Systems



EXPERIMENTATION

AWEs

Division Capstone Exercise (DCX)

Joint Contingency Force (JCF)

Division XXI (DAWE)

Prairie Warrior

BDE TF XXI

Tactical Internet Demo

Warrior Focus

Focus Dispatch

Advanced Warfighting Experiments

ACQUISITION CYCLE

FBCB2

TEST EVENTS

FBCB2 IOTE
FBCB2 LUT3 (NTC)
FT3
FBCB2 LUT2/FDTE
FT2
FBCB2 LUT1
FT1
EPLRS
SINCGARS
NTDR

ATCCS

TEST EVENTS

MCS TT
ISYSCON TT
MCS IOTE
CSSCS IOTE
ASAS BLK II
MSE ATM

First Digitized Division

FIELDING FY00

First Digitized Division

FY 04

DIGITAL CORP

47 Years of Experience

Leaders in Dynamic Test Control, Sim/Stim, Digital Data Capture, with a Systems Approach to Test Design and Data Analysis.

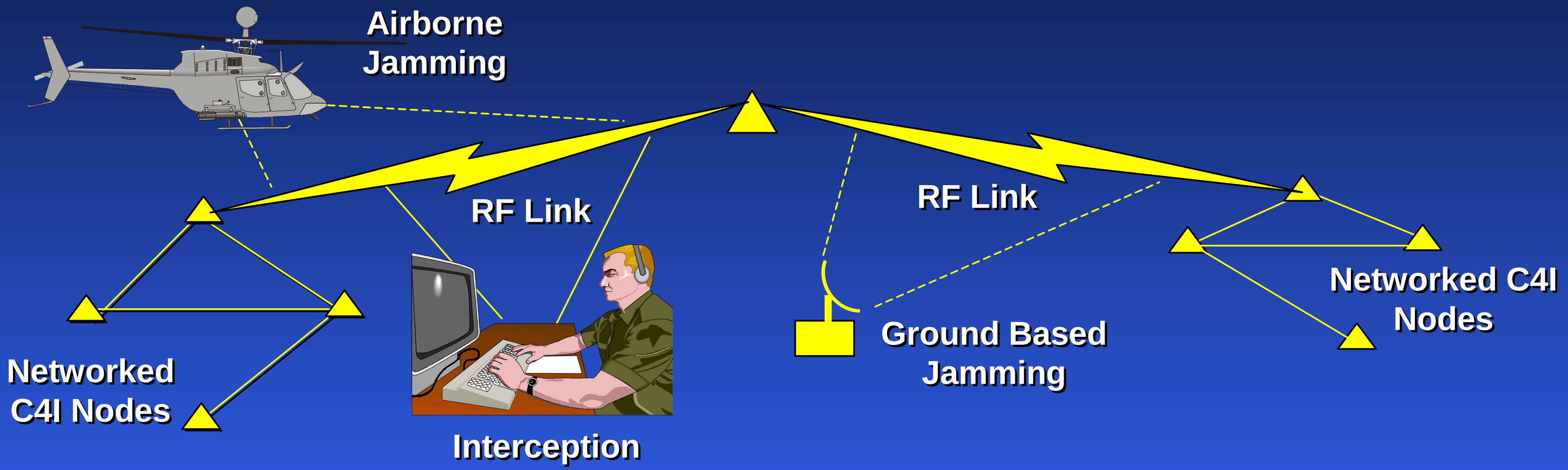
What is Information Assurance?

"Information Operations that protect and defend information and information systems by ensuring their availability, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities."

- Joint Pub 3-13

IA is not SECURITY (But Security is an important IA Subset)

The Old Paradigm – Focus on the RF Links



<u>Things That Deny, Delay, Disrupt and Corrupt Information Flow</u>

- *Jamming*
- *Co-Site*
- *Interception*
- *Xmtr/Rcvr Destruction*

What is the “Threat?”

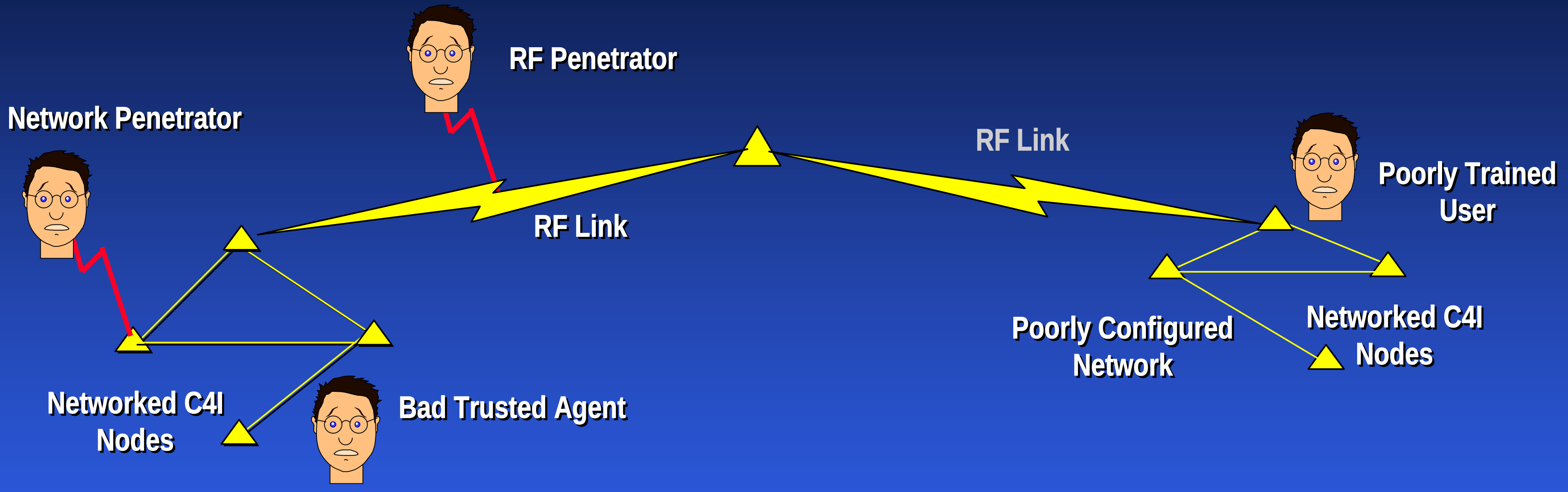
- Sources
  - NSA STAR
  - DISA IASE
  - FBI CyberNotes
- Threat Profile
  - Natural Disaster
  - Power Outages
  - Poorly Configured Equipment
  - Poorly Trained or Error Prone User
  - Bad Trusted Insider (Biggest Single Threat)

----------------------over 80% of threat-------------------------

  - External Hacker
  - Malware (Trojan, Virus, etc.)

Aim is to deny, delay, disrupt, or corrupt information flow thereby denying us information dominance.

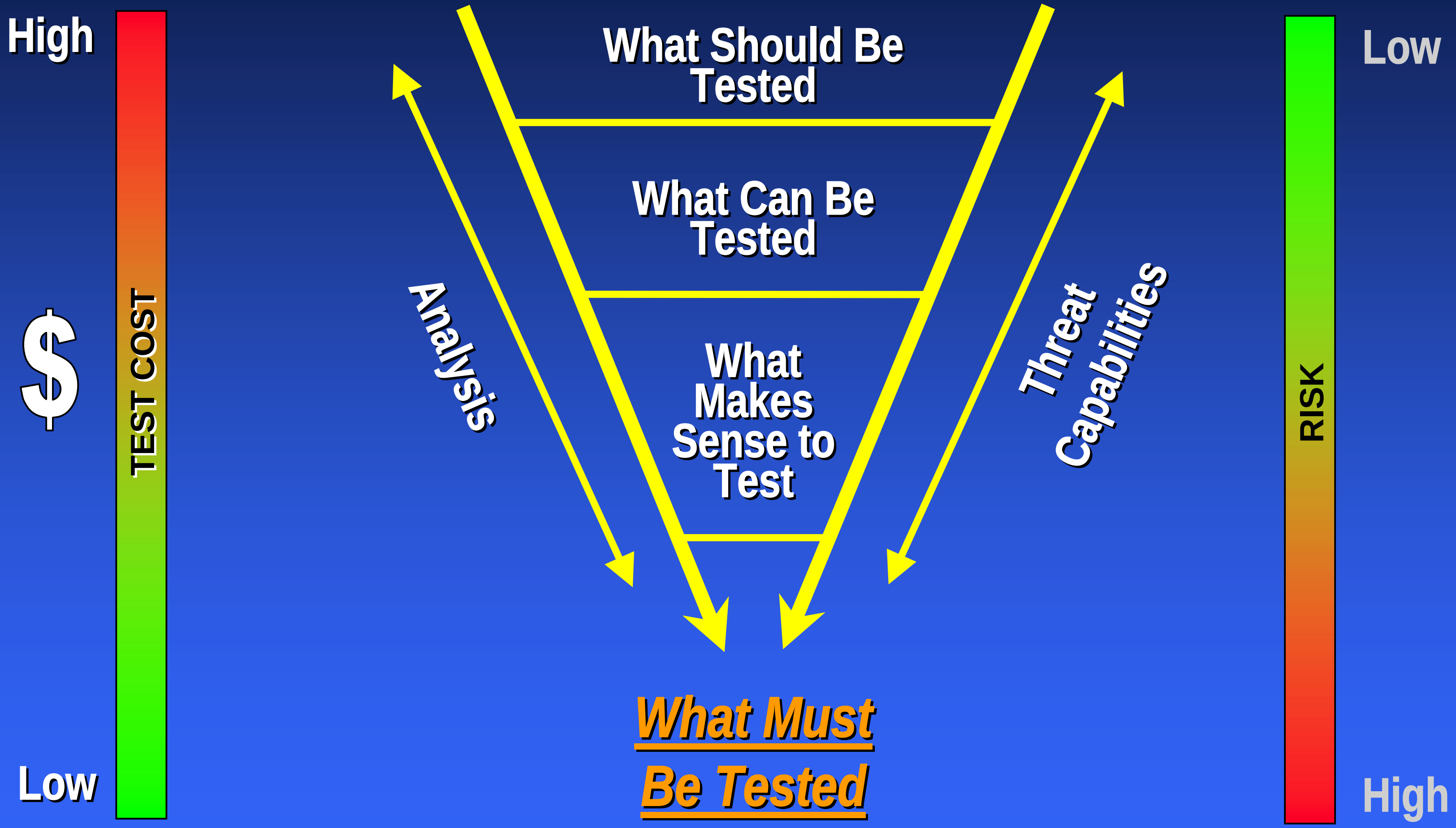
The New Paradigm – Focus on the Networks and RF Links



Things That Deny, Delay, Disrupt and Corrupt Information Flow

- ***Poorly Trained User***
- ***Viruses***
- ***Bad Trusted Agent***
- ***Xmtr/Rcvr/Node Destruction***

Developing a Strategy for IA Testing



High

$

TEST COST

Low

What Should Be Tested

What Can Be Tested

What Makes Sense to Test

Analysis

Threat Capabilities

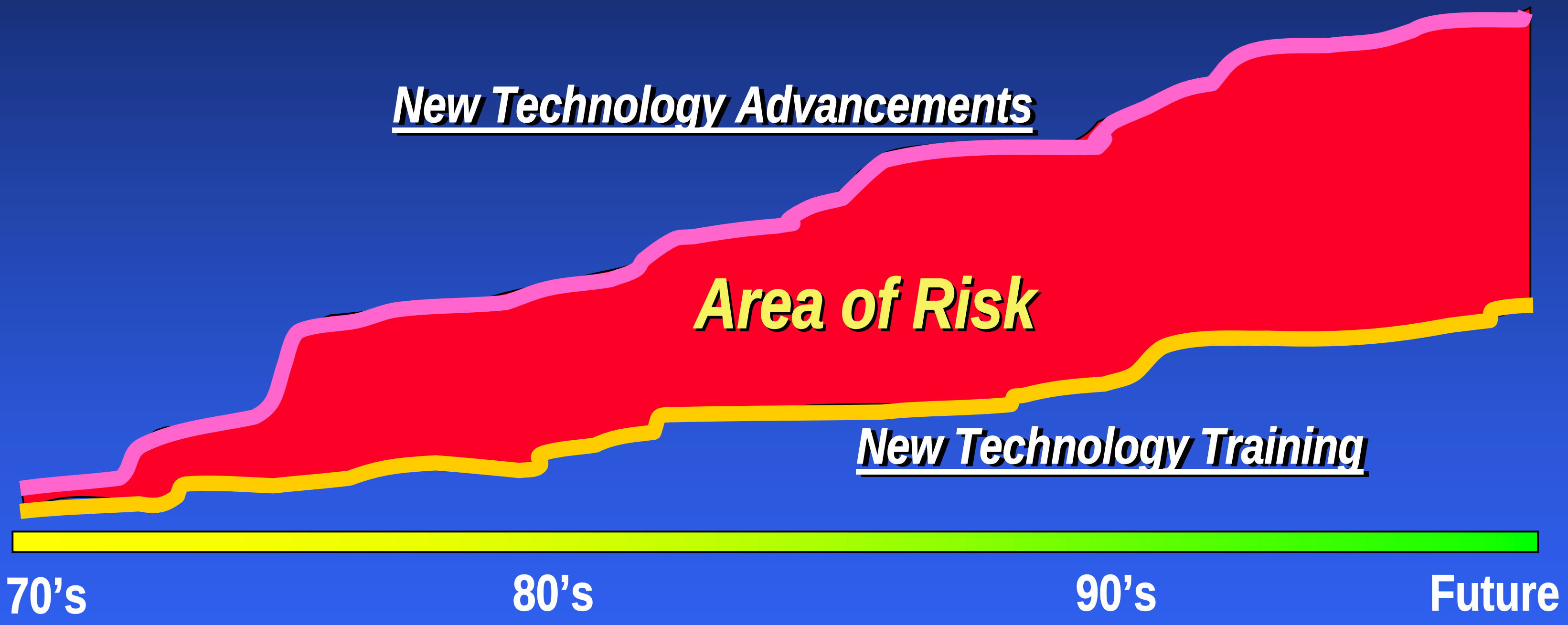
What Must Be Tested

Low

RISK

High

Training Lag



New Technology Advancements

Area of Risk

New Technology Training

70’s

80’s

90’s

Future

Pragmatic Realities Related to IA Testing of a Tactical C4I System

- Should test technical and non-technical elements of IA. However, DiD Architecture, IA procedures, or IA related training may not be in place prior to DT.

- IA MOPs may have been addressed by another test venue (e.g., DITSCAP, JITC, etc.)

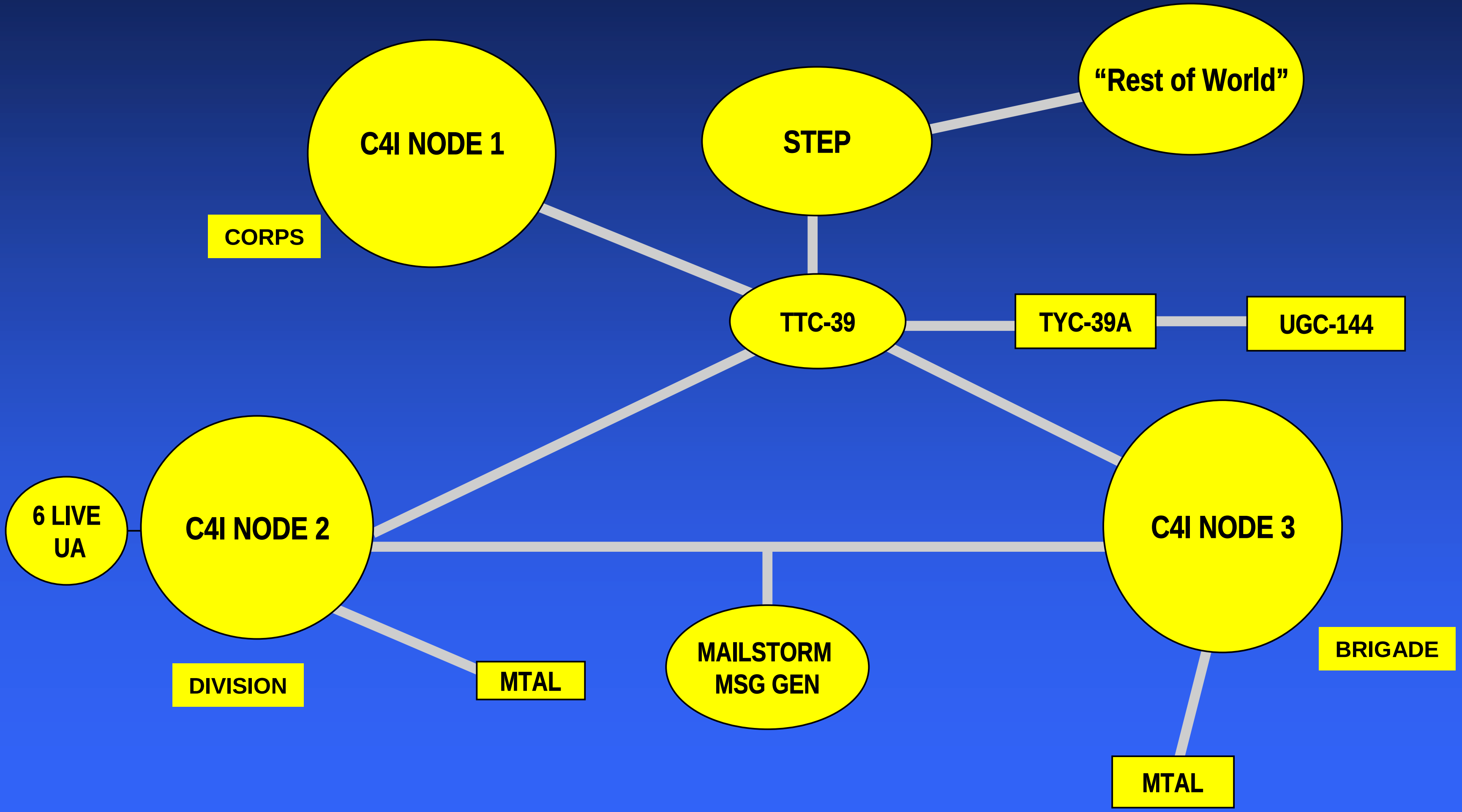
- If a DITSCAP is conducted – before or after DT?

- Programs are short of time and money. How can you afford not to do the “Must Be Tested”?

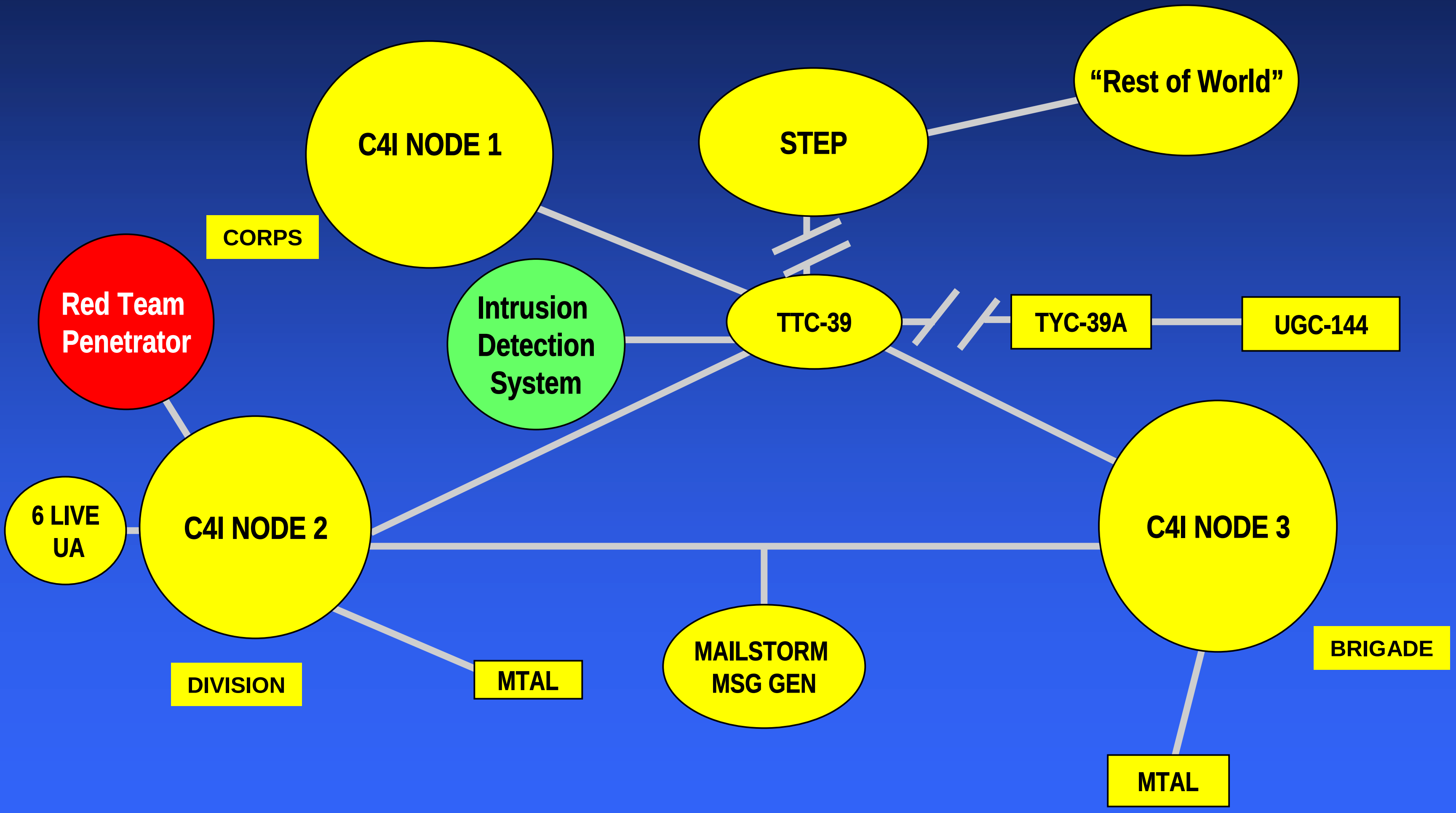
Key Elements in EPG's Approach to IA Testing of Tactical C4I Systems

- Use C-TNOSC as "network monitor"
- Pursue parallel Red Team support from multiple sources (e.g., LIWA and 902nd)
- Added Special Requirements of Virus Testing
  - Conduct at end of Test Window
  - Insure physical isolation of Test Network
  - Protect Test Instrumentation
  - Conduct Post Test system sanitization

Typical Test Configuration - Performance Scenario



IA Test Configuration



Lessons Learned

- Use a “System of Systems” test approach.
- If a DITSCAP is done, then SSAA must be completed in time to support DT/OT planning.
- Cost effective IA Testing requires an integrated Test Strategy
  - Risk assessment, DITSCAP, DT and OT under the construct defined in DOT&E policy (include non-oversight programs).
- IA procedures and trained operators must be developed in a timely manner to support testing
  - DT and DITSCAP Phase II & Phase III offer the best opportunity for testing IA on Tactical C4I Systems.
- IA testing should be approached as a multi-organizational process.