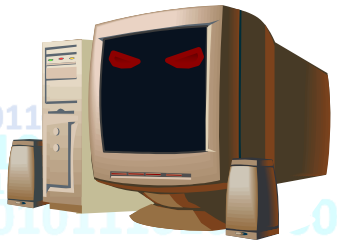
# Getting Better At Not Being Good Enough?

## The State of Cyber Threats and T&E

Brief for ITEA

Baltimore MD 28 Nov 2012

David J. Aland
David.Aland@OSD.mil



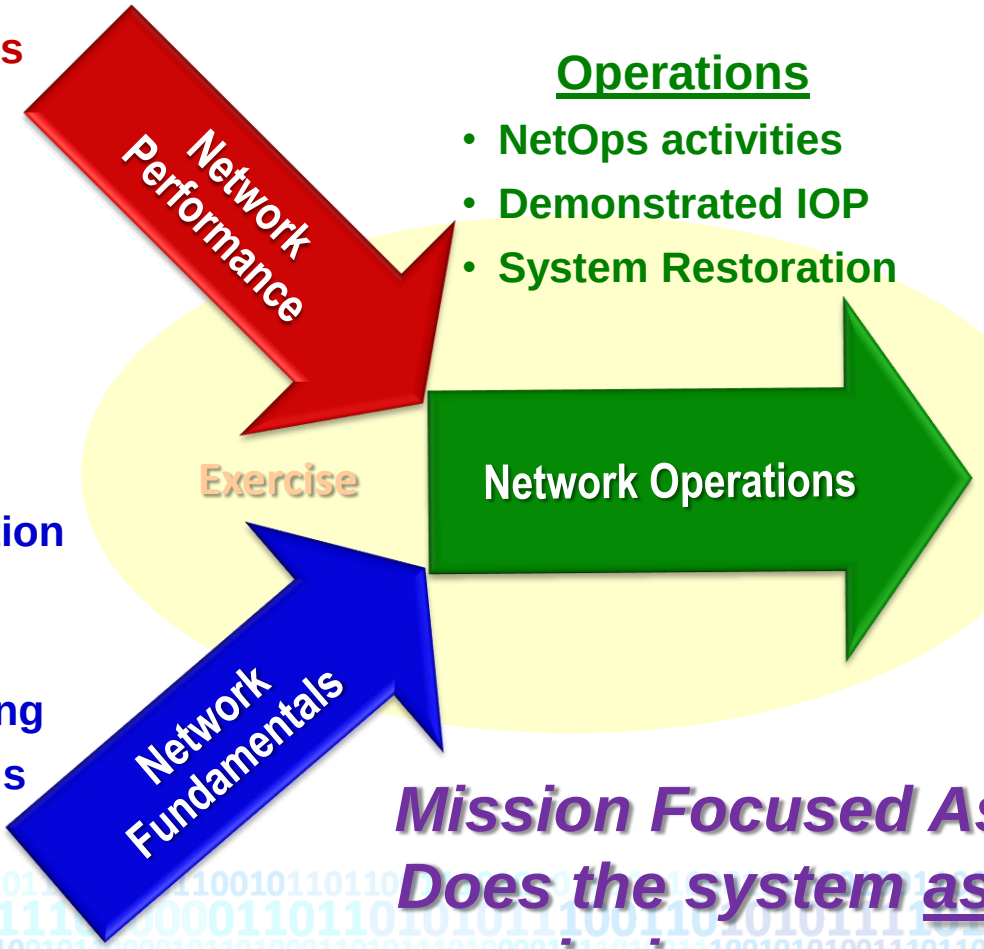
# Cyber T&E Considerations

## Performance

- Red Team Actions and analysis of methods
- Success/Failure
- Detection Rates

## Fundamentals

- Policy/Configuration Compliance
- Best Practices
- Manning & Training
- Processes & Tools
- C&A, IOP Certs




## Operations

- NetOps activities
- Demonstrated IOP
- System Restoration

## Outcomes

- Delays +
- Inaccuracies +
- Inefficiencies +

= RISK to operations

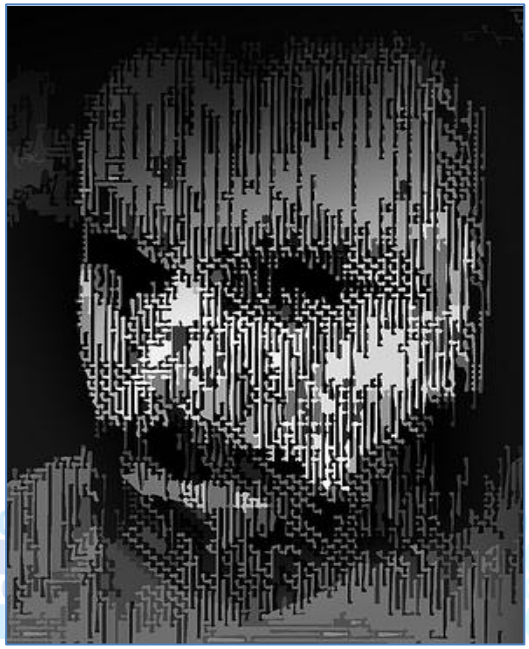
= Mission Assurance (Mission Impact)

***Mission Focused Assessments: Does the system assist or inhibit mission accomplishment?***

# Challenges

- Environment
  - Live vs Memorex
  - Simple vs Complex
- Boundaries
  - System attributes vs “inherited attributes”
  - Threats:  cyber, physical, personnel
  - Back to the Future:  how far ahead?
- New Threat Vectors
  - Physical devices (PWN, Sheeva, etc)
  - Wireless and Bluetooth access
  - Sleeper software, persistent presence
  - In band / out of band management
  - “Poison Pills” (AKA “footshots”)

- How much can you do?
- How many variables can you handle?



# What it Takes

- Safe Sandboxes (ranges, clean networks)
- Realistic threat capabilities
  - Legal permissions, technical skills, tools and personnel
- Test Event Disciplines
  - Designed Experiment, Live-Virtual-Constructive, Sims
- Flexible and frequently updated CAPSTONEs and STARs
- Realistic environmental considerations
  - Not just WHAT the system is expected to do
- Comprehensive Interoperability reviews and certs