

# Simulation Needs for Cyber Analytics

1100 EDT

16 October

# Introduction

- Simulation Group Leads
  - Sandy Thompson
  - Laura Nolan

# Overview

- One of the Discipline Groups
- Group will
  - examine the analytical issues from the tracks
  - Identify issues that simulation can help address
  - Propose simulation solutions to address issues
- DCO session goal is to identify
  - Current capabilities
  - Requirements
  - Capability needs
  - General Information

# Please rate (high, med, low) how Simulation is doing in...

Tracks	Overall	Well defined need	Requires research	Importance	
Cyber Environment & 4 <sup>th</sup> Gen					
Cyber Situational Awareness & C2					
Cyber Defense					
Cyber Exploitation and Offensive Ops					
Cyber Deterrence					
Cyber Impacts to Business					

# Current Capabilities

- What are current simulation tools?
- Characteristics of good tools
  - Fidelity
  - ease of use,
  - cost, ...
- Should tools be accredited by IO JMEMS?
- What sort of V&V is/should be required for Cyber Simulation tools?

# Simulation Questions

1. What variables need to be accounted for in simulations?
  - Human interfaces with networks
  - Applications
  - Data packets
  - Data flows
  - Network characteristics (bandwidth, routes, ...)
  - Defensive countermeasures
  - Adversary activities
  - Mission impact

# Simulation Questions

2. What systems should be simulated and where?

- Computer network
- Critical Infrastructures
- Process control systems
- Others
- On the IO Range,
- Other ranges and testbeds

# Simulation Questions

3. Who is the target audience for cyber simulations?
  - Network/Software/Hardware designers
  - Network builders
  - System Administrators
  - Cyber Ops Planners
  - Cyber Ops Decision makers
  - End-host Users
  - Business managers
  - ...

# Requirements for Simulation Tools

- What sets of requirements are applicable?
- What requirements should be added?

# Needed Capabilities

- Areas in need of simulation
- Prototype Tools
- Accreditation process
  - What should be included
  - Who should lead or participate

# General Needs

- Identify organizations who fund cyber simulation research
- Identify organizations who do or would be interested in cyber simulation research

What are we missing?