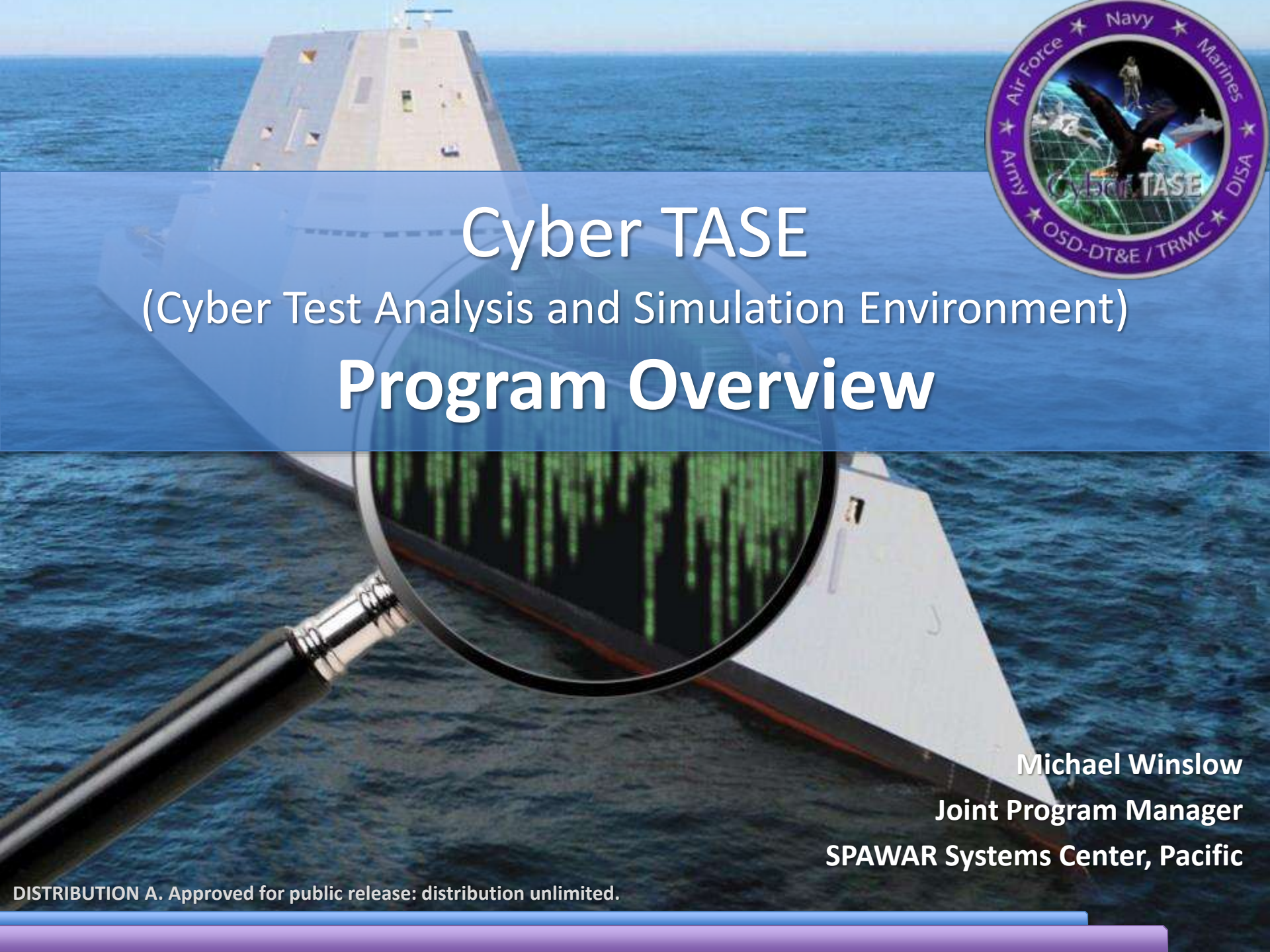


Cyber TASE

(Cyber Test Analysis and Simulation Environment)

Program Overview

Michael Winslow

Joint Program Manager

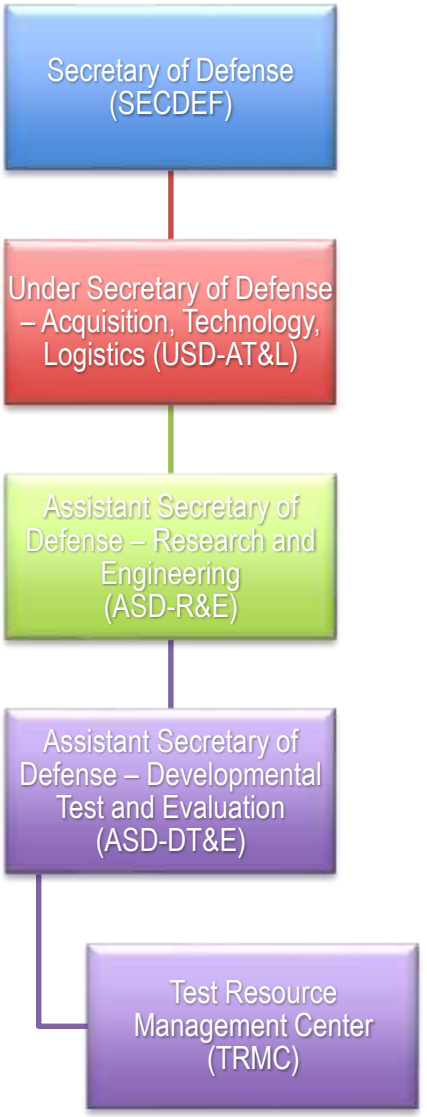
SPAWAR Systems Center, Pacific

Army
Air Force
Cyber TASE
Navy
DISA

Sponsor Overview

Department of Defense
DASD-DT&E / TRMC
CTEIP

- ASD-DT&E (Developmental Test and Evaluation)
  - Provides oversight over DT
- TRMC (Test Resource Management Center)
  - Strategic planning of Testing Ranges
  - Reviews and certifies T&E Budgets
  - **Runs the Centralized T&E Improvement Program (CTEIP)**
  - Runs the T&E S&T Program
  - Runs the Joint Mission Environment Test Capability (JMETC) Program

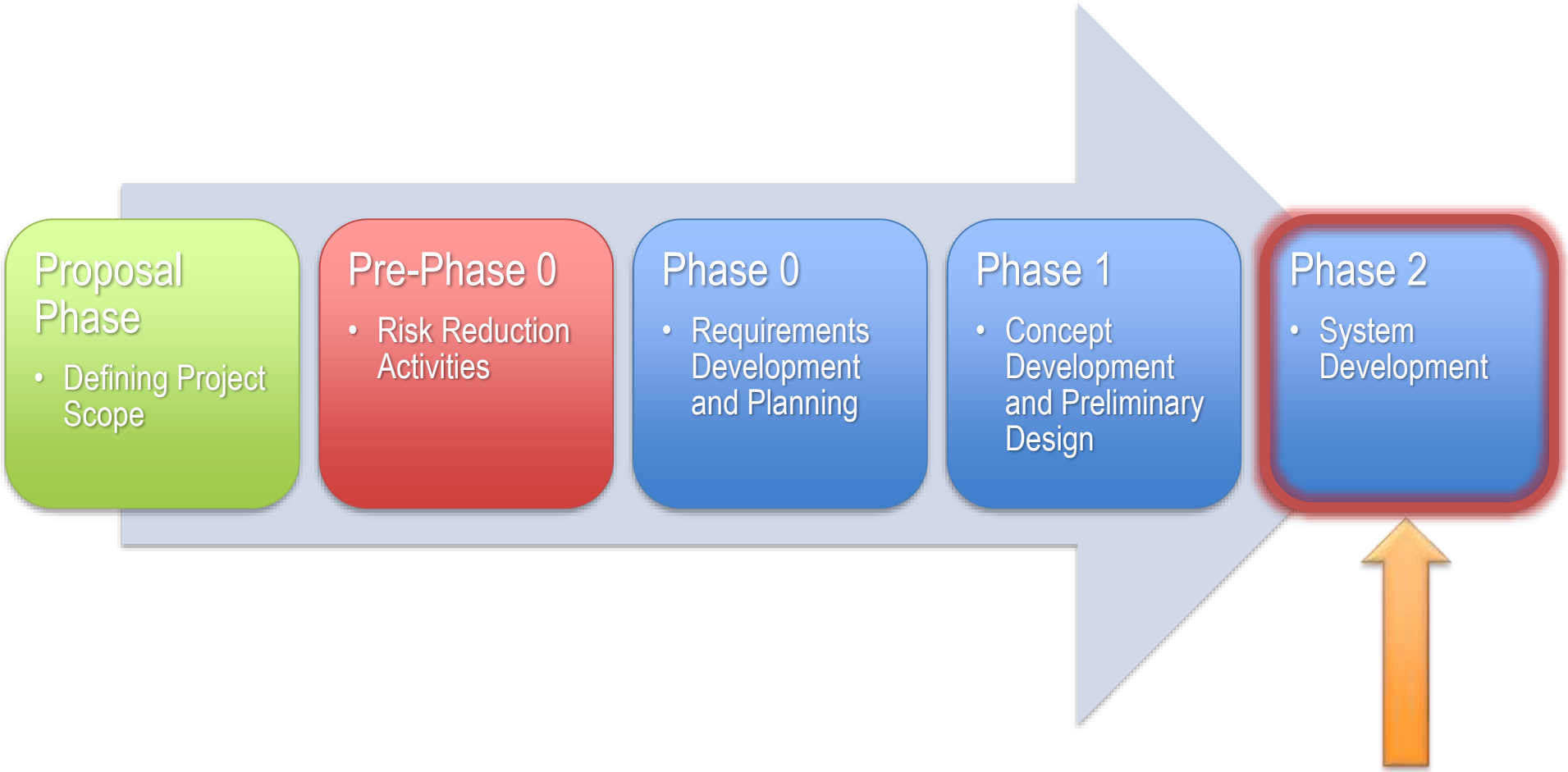


Army
Air Force
Cyber TASE
Navy
DISA

CTEIP Program Process

Department of Defense
DASD-DT&E / TRMC
CTEIP

1-2 years | 0.5 – 1 year | 1-2 years | 3-4 years



Army

Air Force

Cyber TASE

Navy

DISA

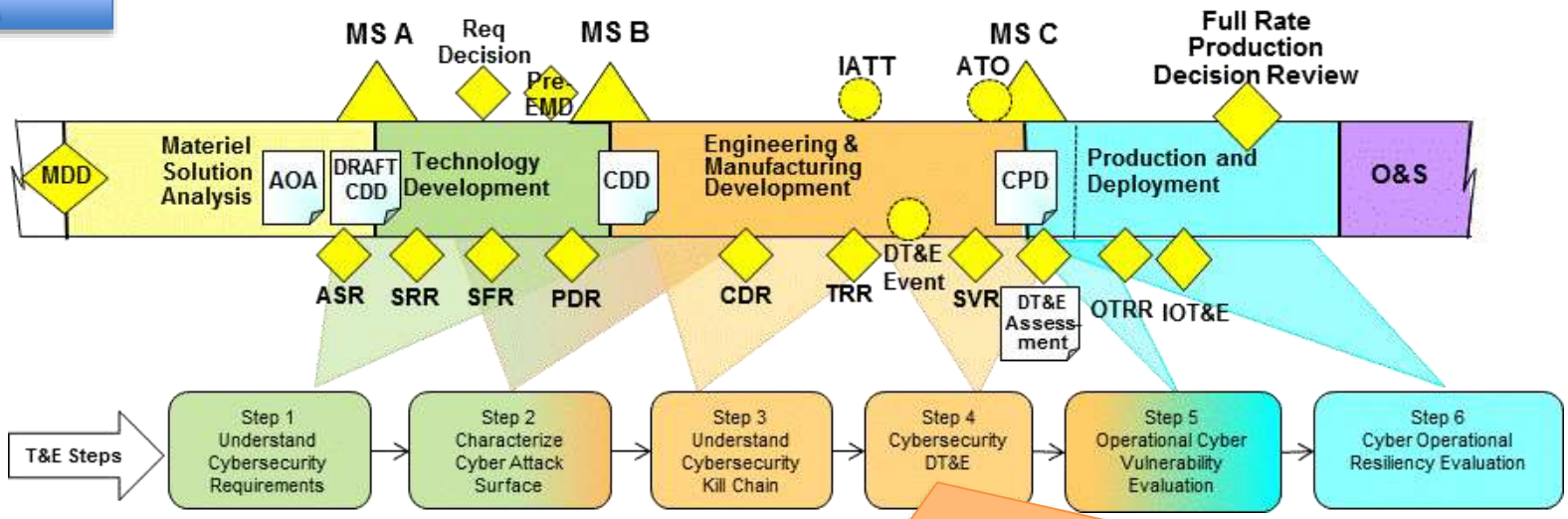
Department of Defense

DASD-DT&E / TRMC

CTEIP

Cyber Test Requirements

Developmental Test



Step 4. Conducted before Milestone C, Step 4 is an end-to-end assessment in a representative mission context for the system under test in order to evaluate the readiness for limited procurement/deployment and operational testing. This step focuses on conducting a rigorous cybersecurity/IA test in as realistic an environment as available, and requires the use of a threat-representative test team (Red Team) in testing the potential and actual impacts to the system. Results of the Red Team testing will be included as part of the DT&E Assessment. Programs (depending on risk) may want to consider using a cyber range to reduce the risk of potential collateral damage to live networks and authoritative data sources in order to analyze the impact to the system mission in a cyber-contested environment. For major defense acquisition programs, major automated information systems, and those programs on the AT&L Special Interest list, DASD(DT&E) will include a cybersecurity/IA analysis within the DT&E assessment in support of Milestone C. Shortfalls identified in this and previous steps should be resolved prior to proceeding to OT&E, and programs should plan for sufficient time and resources for these resolutions.

Cyber TASE will greatly aid in the analysis required to satisfy Step 4 of the draft "6 Step Process" required for IA testing of C4I and Enterprise Acquisition Programs.

Army

Air Force

Cyber TASE

Navy

DISA

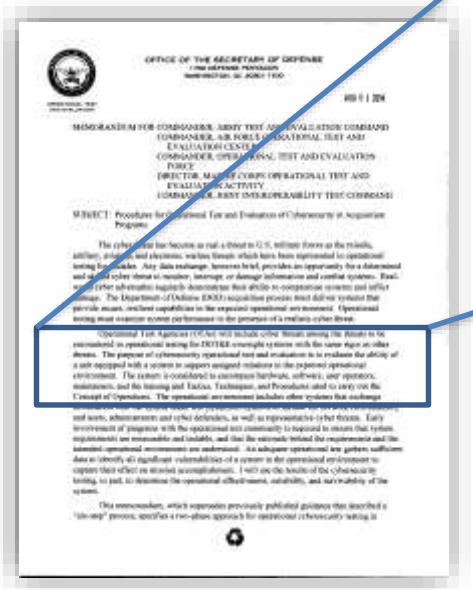
Cyber Test Requirements

Operational Test

Department of Defense

DASD-DT&E / TRMC

CTEIP



Memorandum from Dr. J. Michael Gilmore (DOT&E)

"All oversight systems capable of sending or receiving digital information are required to conduct cybersecurity testing. This includes uploading or downloading data by physical means such as Universal Serial Bus (USB) connections or removable data devices."

Phase 1: Cooperative Vulnerability and Penetration Assessment

The purpose of this phase is to provide a comprehensive characterization of the cybersecurity status of a system in a fully operational context, and to substitute for reconnaissance activities in support of adversarial testing when necessary

Phase 2: Adversarial Assessment

This phase assesses the ability of a unit equipped with a system to support its missions while withstanding validated and representative cyber threat activity.

Cyber TASE will greatly aid in the analysis required for both Phases of the OSD-DoT&E Cybersecurity Test Memo levied upon acquisition programs.

Army
Air Force
Cyber TASE
Navy
DISA

Department of Defense
DASD-DT&E / TRMC
CTEIP

Project Description

- Description
  - Distributed engineering test capability to assess Cyber Impacts on the ability of the SUT to perform in a Cyber contested environment.
- Key Characteristics
  - Provides integrated instrumentation for collecting, analyzing, and visualizing the test data across multiple layers/sources to understand the mission impacts of the Cyber threat.
  - Provides constructive simulation to scale L-V-C environment to be able to represent a full scaled operational environment and the impact of Cyber threats on conducting mission operations.
- Core Capabilities Developed

Instrumentation	Constructive Simulation	Demonstration
➢ Enhancements to data collectors to provide ease of use, consistency, and to integrate to other capabilities. ➢ Analysis and Visualization environment to provide near-Real-Time and Post-Test Analysis and Visualizations.	➢ Adding in CND Models, creating network palettes for quick model creation, library of pre-defined attacks with easy user configurability, creating visualization environment. ➢ Integration into the Instrumentation Suite for L-V-C Testing.	➢ Conducting a demonstration for each of the three incremental deliveries. ➢ Will be growing in scope each year to include additional Services. ➢ Will be growing in scope each year to cover more Use Cases in subsequent years

Army
Air Force
Cyber TASE
Navy
DISA

Alignment within TRMC Cyber Test Capabilities

Department of Defense
DASD-DT&E / TRMC
CTEIP

Infrastructure

National Cyber Range

- Test Hosting Environment for Key Slices of a Larger Architecture
- Rapid Test Setup / Sanitization
- Toolset for Defining Environment

STEALTHNET

- Scalable Simulation Environment with a Real-Time Hardware-in-the-Loop Capability
- Army Use Case Oriented, focused on S&T
- Limited threat modeling and analysis capabilities

L-V-Constructive

Cyber TASE

- Provides integrated instrumentation for collecting, analyzing, and visualizing the test data across multiple layers/sources to understand the mission impacts in a Cyber contested environment.
- Provides constructive simulation to scale L-V-C environment so we can represent a full scaled operational environment and the impact of Cyber threats on conducting mission operations.

Transport

JMETC MILS Network & RSDPs

- Provides Isolated Inter-Lab Transport
- Replacing JIOR for Test
- Provides Cloud Services for Test
- Small & Modular Test Hosting Environment

InterTEC

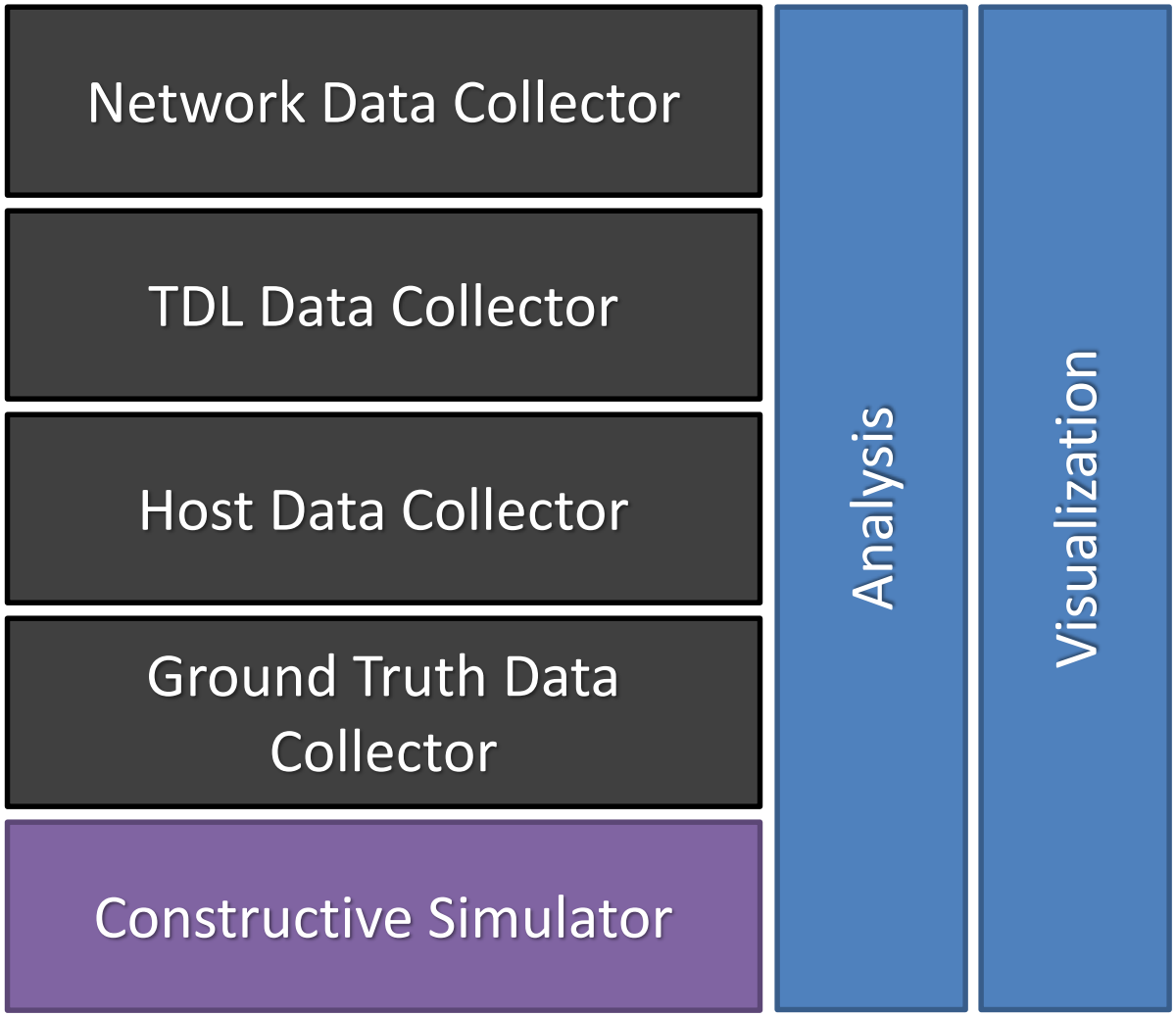
- Focus on TDL & AOC Interoperability
- Development of Tactical Data Link Instrumentation

Instrumentation

Army
Air Force
Cyber TASE
Navy
DISA

Cyber TASE Functional Domains

Department of Defense
DASD-DT&E / TRMC
CTEIP



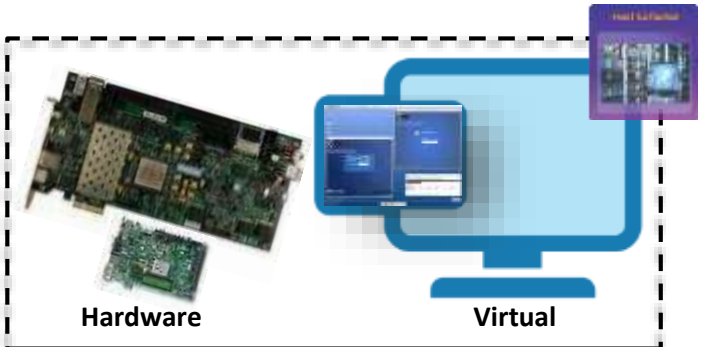
Army
Air Force
Cyber TASE
Navy
DISA

Department of Defense
DASD-DT&E / TRMC
CTEIP

Project Deliverables

Network and Host Data Collectors

Network Hardware Collector and **Remote Host Collector**



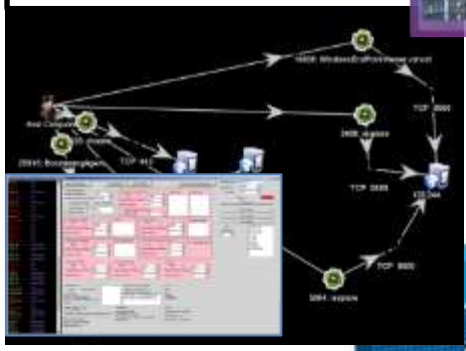
High Fidelity Host Data Collector

Provides Data

Remote Connect via SSH

Network Data Collector

Deployable Host Collector



Remote Host Collector

Windows SysInternals

The Network Data Collector will run GOTS software on a Server and can tap up to 4 network ports. The Remote Host Collector process will run on this appliance and the deployable (installed) agents will feed data back to the network collector. The High Fidelity Host Collector will support detailed process and memory analysis required to do detailed Cyber test.

Army
Air Force
Cyber TASE
Navy
DISA

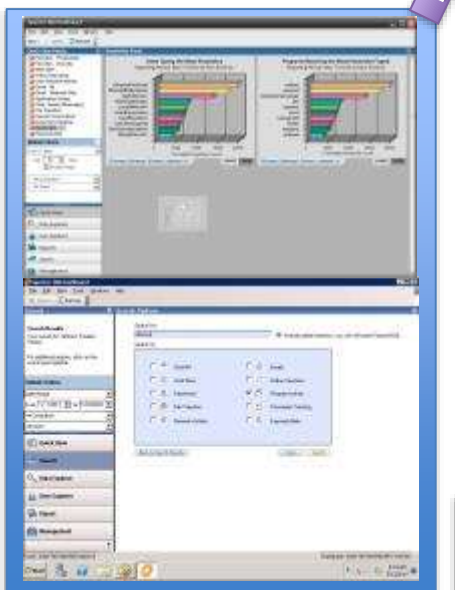
Project Deliverables
Ground Truth Data Collectors

Department of Defense
DASD-DT&E / TRMC
CTEIP

Ground Truth Collector Hardware and Storage

Provides Data

Provides Data



Log Files – Keylogging – Chat

VoIP Call Recording

Screenshots
(Software + Hardware)

Threat Representation Team

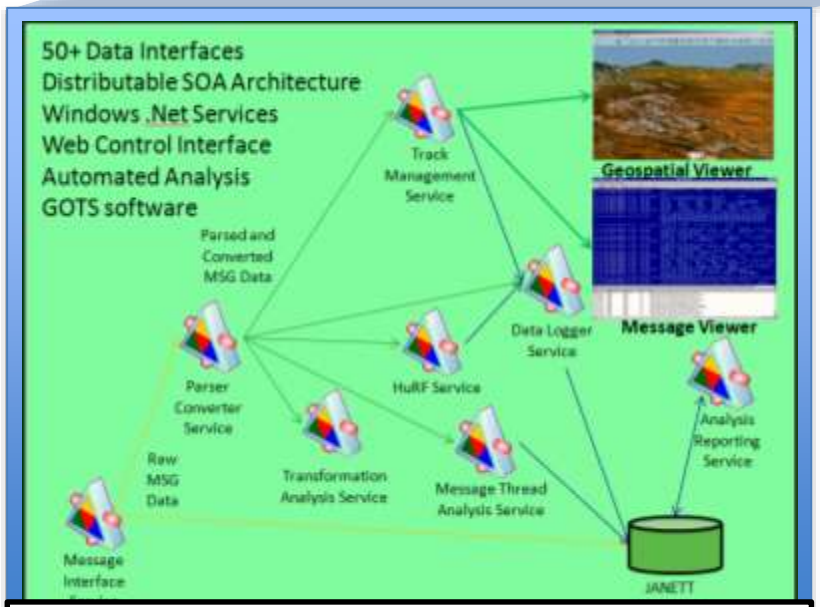
The Ground Truth (GT) data collector is fed by several different sources. Logs and Keylogs are extracted from user workstations and NETT events from NETT Web Services are fed to the GT Server. The GT Server will have a port in the Voice VLAN to intercept and record test teleconferences. Screenshots can be collected via hardware or software agents and will be fed to the local GT Server.

Army
Air Force
Cyber TASE
Navy
DISA

Department of Defense
DASD-DT&E / TRMC
CTEIP

Project Deliverables

TDL Data Collectors



JANETT

NSITE

Similar to the Network Collector, a TDL Data Collector will be installed on the network to capture JREAP-C (Link 16) messages and to process them for inclusion in the analysis. Two capturing tools will be available, JANETT, which provides the data analysis engine and NSITE, which contains a cross-site correlator and visualization.

Army
Air Force
Cyber TASE
Navy
DISA

Department of Defense
DASD-DT&E / TRMC
CTEIP

Project Deliverables
Data Collection

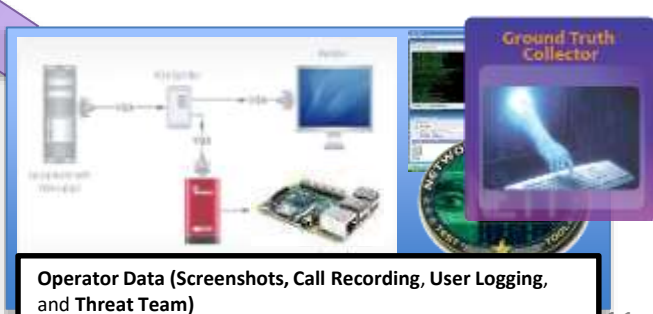
Network Hardware Collector and **Remote Host Collector**

TDL Hardware Collector

Ground Truth Collector Hardware and Storage

Network and Host

Tactical Data Link



Operator Data (Screenshots, Call Recording, User Logging, and Threat Team)

The Network, Host, TDL, and Ground Truth Data Collectors are composed of the best-of-breed data collectors. They will be installed at Service Labs and the NCR. They are readily deployable to additional labs as necessary.

Army

Air Force

Cyber TASE

Navy

DISA

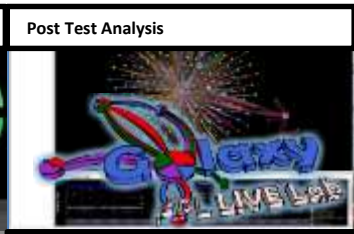
Project Deliverables

Integrated Services

Department of Defense

DASD-DT&E / TRMC

CTEIP

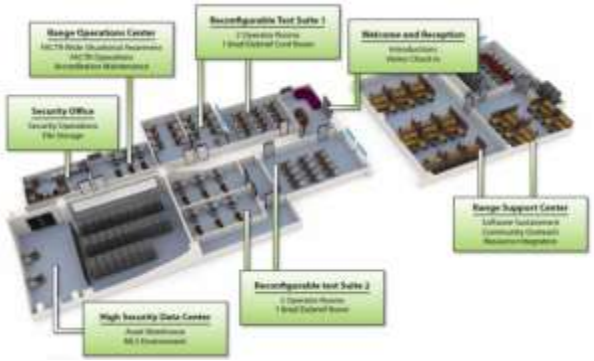


Cyber TASE Integrated Services

The Visualization, Analysis, and Constructive Simulator form the Cyber TASE Integrated Services, which will be installed at the TRMC provided Regional Service Delivery Points (RSDPs) to be accessed via the JMN, at the National Cyber Range, or via a Portable Node.

Regional Service Delivery Points

National Cyber Range



Portable Node

Army

Air Force

Cyber TASE

Navy

DISA

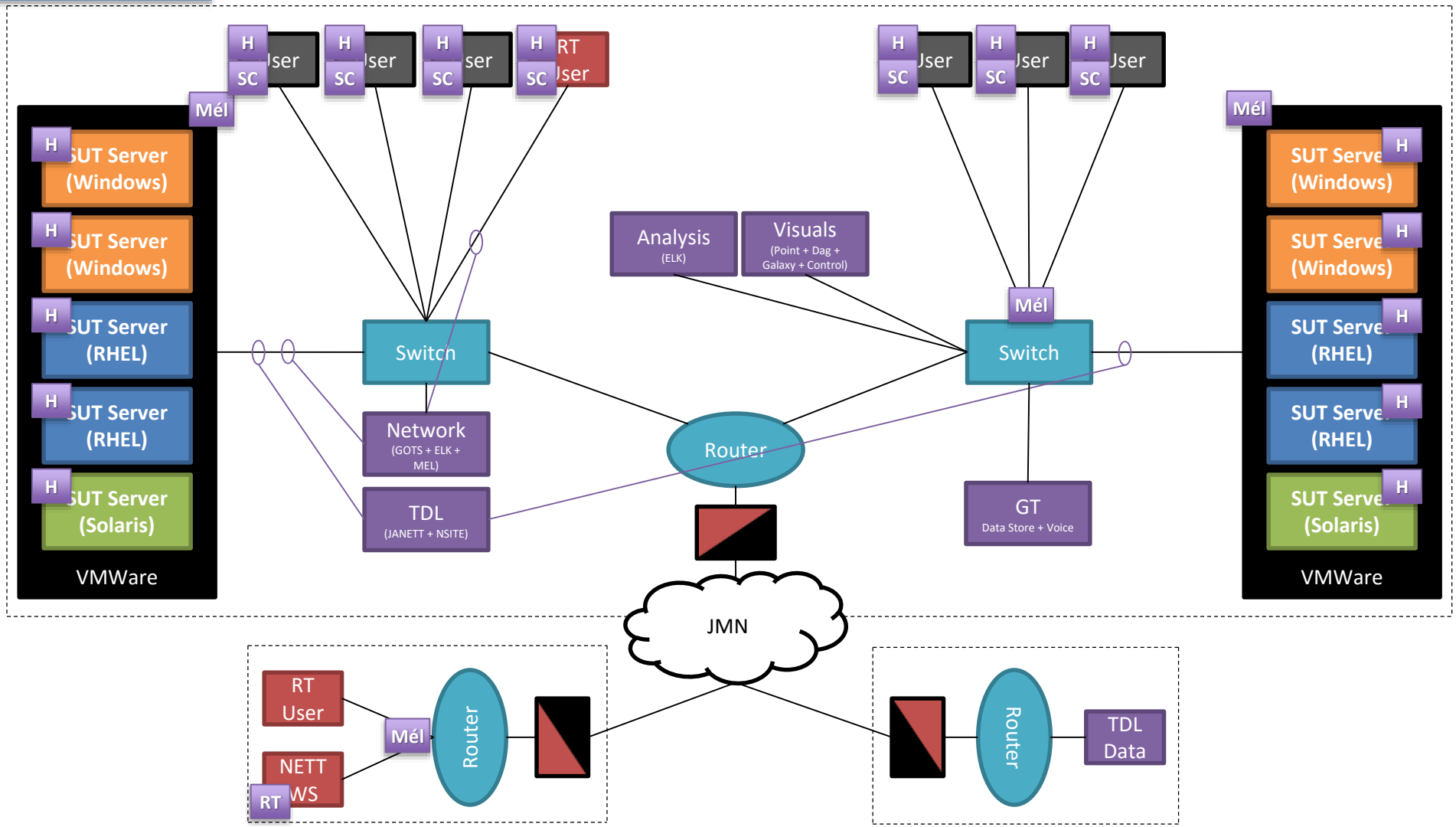
TASE Overall System

Data Collection, Analysis, and Visuals

Department of Defense

DASD-DT&E / TRMC

CTEIP



Army
Air Force
Cyber TASE
Navy
DISA

Schedule and Budget

Department of Defense
DASD-DT&E / TRMC
CTEIP