Threat Cyber T&E

Skip Tornquist
Technical Director
Threat Systems Management Office (TSMO)
COM (256) 876-8565
DSN 746-8565
Skip.tornquist@us.army.mil

14 September 2011

Threat Cyber T&E

- Validated, accredited, Threat Computer Network Operations (CNO) teams (personnel and tools) executing Computer Network Exploitation (CNE), Computer Network Defense (CND) and Computer Network Attack (CNA) in support of T&E.
  - Four major Threat levels ranging from lone, amateur operators to nation-state Threats.
  - Threat CNO Tactics, Techniques, and Procedures (TTPs) and the tools to employ them.
  - Integrated with and C2 as part of the overall Threat force.
- Persistent Threat environment.
- Represented in Live, Virtual, and Constructive (LVC) domains at multiple levels of security classification.

Levels of Threat

Level 1

- Lone or small group actors
- Common tools, techniques
- Unsophisticated without significant support

Level 2

- Individuals or small groups supported by commercial entities, criminal syndicates, or other transnational groups such as terrorist networks
- Common tools used in a sophisticated manner
- Activities include espionage, data collection, network mapping/recon, and data theft

Level 3

- Individuals or small groups supported by state-sponsored institutions (military or civilian)
- Significant resources and sophisticated tools
- Activities include espionage, data collection, network mapping/recon, and data theft

Level 4

- State-sponsored offensive IO especially CNA
- State-of-the-art tools and covert techniques
- Activities conducted in coordination with military operations

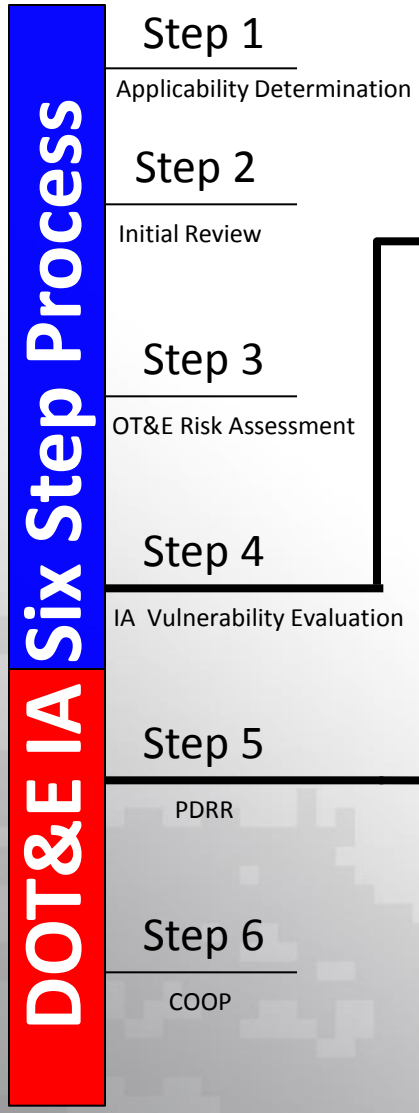
What is Threat CNO ?

- **Computer Network Operations (CNO)**
  - Computer Network Defense (CND)
  - Computer Network Exploitation (CNE)
  - Computer Network Attack (CNA)
- **Threat CNO is an information operations activity, supporting a threat commander's objectives.**
  - Defined Threat
  - CND - Requires Threat CND
  - CNE - Requires not only identification of further means of technical or physical compromise, but exploitation of data to support threat commander's objectives.
  - CNA - May require denial of service, degradation of capabilities/systems, software/hardware destruction via computer attack.

Penetration Testing

- **If that is Threat CNO, what is penetration testing?**
  - Technical exercise that verifies the application and effectiveness of specific information assurance (IA) protective measures of systems.
  - Prevents unauthorized access to computer systems by identifying points of unauthorized access, assessing depth and degree of potential compromise, and recommending methods, techniques, and configuration modifications needed to secure the system.
  - No defined adversary
  - No threat CND
  - Minimal CNE
  - Minimal CNA – no denial, no degradation, and no destruction

OT&E of IA in Acquisition Programs



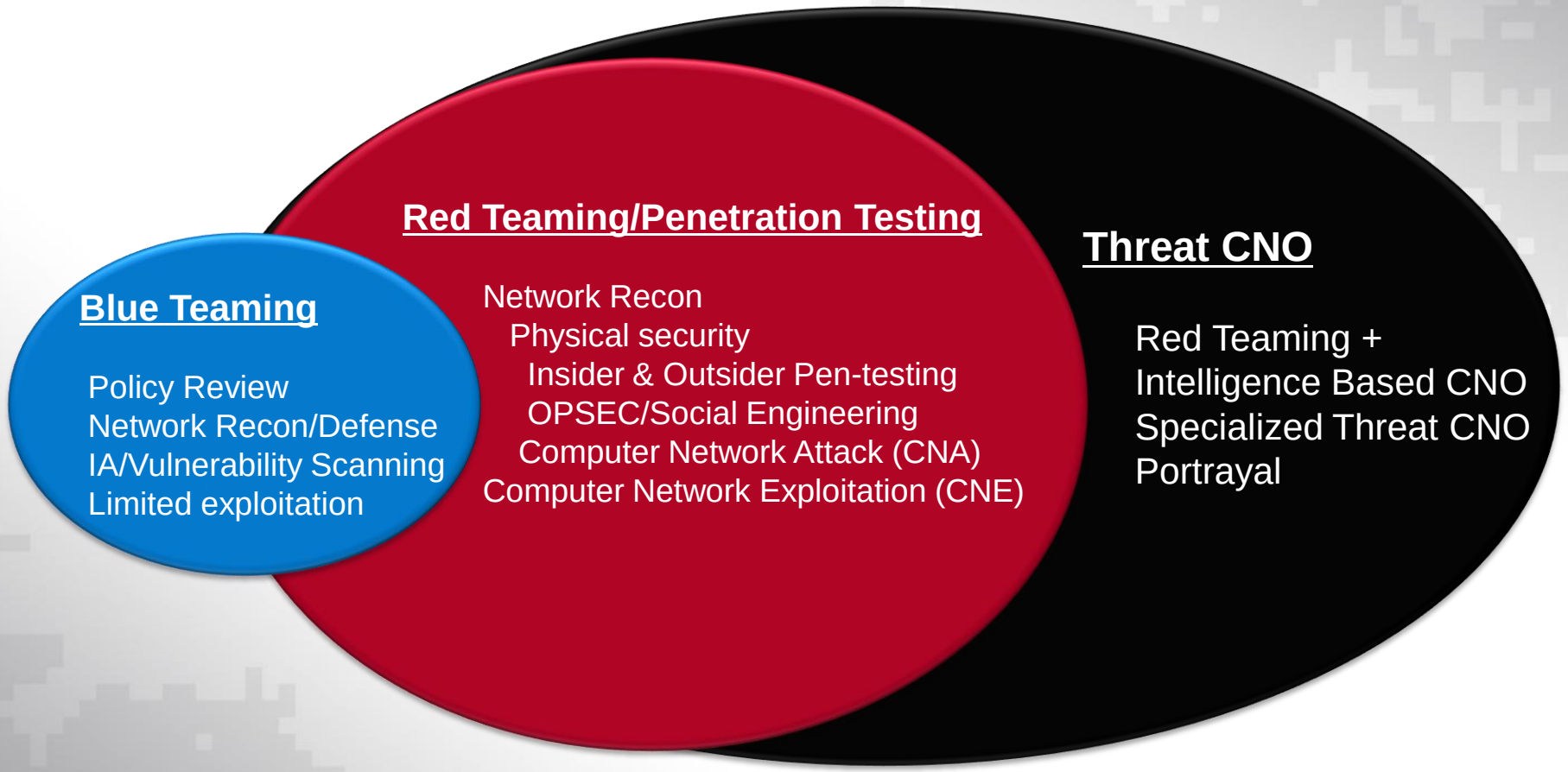
Vulnerability Assessment in support of C&A

- Evaluation of inherited controls from the C&A Process
- Patch Management and network access controls
- Provide vulnerability evaluation to materiel developer
- Leverage as much DT data as possible
- Limited penetration testing to support verification of vulnerability scan findings

TCNO Capability Required

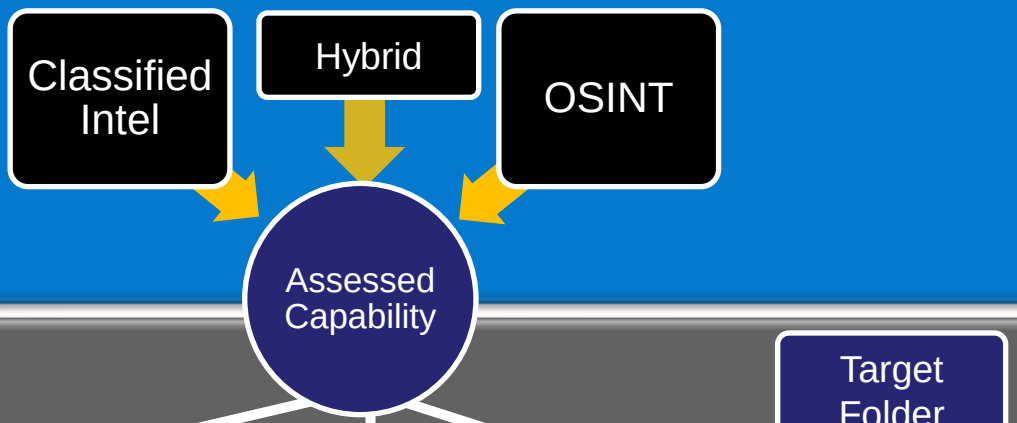
- Independent and comprehensive evaluation of PDRR
- Threat-based approach using accredited and validated threat
- Realistic, system-of-systems, operational environment
- Includes aspects of penetration testing, red teaming, and threat-based computer network operations
- Verifies step four findings as necessary to test PDRR
- Threat objective based testing designed to accomplish realistic OPFOR goals

Threat CNO Concept



Level 1 → Level 2 → Level 3 → Level 4

Threat Portrayal Process



TARGET RESEARCH & ANALYSIS

Open & Closed source target research and analysis is conducted to determine appropriate associated threat and capabilities. Hybrid sources may include just-in-time training to learn complex systems or the use of unique internal analysis tools.

DOCUMENT & DEVELOP

Threat team composition & tool selection is based on target analysis results. A target folder consisting of a wide array of target-specific facts & threat portrayal findings is derived.

VALIDATE & ACCREDIT

Determined threat portrayal is validated for realism annually and accredited for suitability prior to each sanctioned event.

APPLY

Threat tools & techniques are applied in a manner within the scope of pre-established rules of engagement.

Threat Cyber T&E – The Way Ahead

- Threat Cyber must be part of a Cyber "Major Range and Test Facility Base (MRTFB)"
  - Persistent Threat Services (Threat CNO and Environments)
  - Integrated with the IO Range services and connectivity
  - Distributed to the Cyber MRTFB sites
  - Support Service, Joint, and Coalition T&E, training, and experimentation
- Threat Cyber development must keep pace as acquisition and testing evolves
  - Included early on in T&E planning
  - Supports agile acquisition process
    - Army Force Generation (ARFORGEN) and Network Integration Evaluation (NIE)
  - Employed in Live, Virtual, and Constructive (LVC) domains .
- Threat Cyber must have dual-use capabilities

PERSISTENT THREAT CYBER IS A FULL TIME MISSION

Questions

Questions