**NDIA Hard Problems Workshop Cyber COI Deep Dive (U)**

**AFRL/RI, 525 Brooks Rd, Rome NY 13441-4505**

**Approved for public release, distribution unlimited**

**The original document contains color images.**
NDIA Hard Problems Workshop - Cyber COI Deep Dive

5 Nov 14

Dr. Richard Linderman
Cyber COI Steering Group Lead

This briefing is Approved for Public Distribution. OSD Release #14-S-2118
Outline

- BLUF
- Cyber COI Overview
  - Roadmap Development Process
  - Cyber COI “4 + 2” S&T Roadmaps and Recent Successes
  - Hard Problems and Gaps
  - Engagements, Way Ahead, and Opportunities
- Summary
BLUF – Bottom Line Up Front

- Established, mature, and coordinated community

- Cyber S&T aligned to expanding operational capability gaps/priorities

- Cyber S&T contributions to nearly all Seven DoD Hard Problems

- Driving deeper engagement with industry and international partners
S&T Influencing the DoD Cyber Landscape

"...we will continue to invest in capabilities critical to future success, including... operating in anti-access environments; and prevailing in all domains, including cyber."

- President Obama, January 2012
DoD Cyber S&T Coordination

ASD(R&E) Oversight

Research Directorate

Cyber S&T Community of Interest (COI)

**Cyber Coordination Team**

Special Cyber Operations Research Engineering (SCORE) Interagency Working Group

Networking and Information Technology Research and Development (NITRD)

Cyber Security and Information Assurance (CSIA) Interagency Working Group

- **COI Steering Group:**
  - **SG Lead:** AF - Dr. Richard Linderman
  - **Deputy:** Army - Mr. Henry Muller
  - Navy - Dr. Wen Masters
  - NSA - Dr. Boyd Livingston
  - OSD - Dr. Steven King

- **COI Working Group:**
  - **WG Lead:** AF - Mr. Chester Maciag
  - **Deputy:** Army - Mr. Giorgio Bertoli
  - Navy - Dr. Gary Toth
  - NSA - Mr. Grant Wagner
  - OSD - Mr. Stephen Luther

**Users**
- DISA
- NSA IAD
- DCIO
- ONR/NRL
- AFR/AFOSR
- NSA Research
- DARPA
- RDECOM
- DTRA
- USSTRATCOM/USCYBERCOM
- USD(I)

**Research Community**

Community of Interest and Working Groups are the primary means for oversight, collaboration, & coordination

Distribution A – For Public Release
Cyber COI - Scope

An Operational Domain: JS OV-5a. Based on JROC-Approved Capability Documents and DoD CIO-developed Architectures

- Spans Defense, Effects, Situational Awareness-Course of Action
- Includes enterprise, tactical and embedded
- Cuts across all domains
- Touches C4I, EW, Autonomy, and Human Systems COIs
- Transcends S&T across all DOTMLPF
- QDR Tenets Addressed
  - Mitigates Threats
  - Delivers Affordable Capability
  - Affords Technological Surprise
DoD Cyber S&T: Performers
(FY14 Execution)

- Service S&T Labs
  - AFRL, RDECOM, NRL, SPAWAR
- DoD Agencies
- DoE Labs
- FFRDCs
- Industry
- Academia

Breakout by Recipient (%)

- Academic
- Industry
- FFRDCs
- DOE Labs
- DoD S&T Lab
Cyber COI Recent Activities

- (U) Briefed roadmap to S&T EXCOM in May
  - (U) Cyber PSC → Cyber [Security] COI
  - (U) Incorporated findings of Cyber Investment Management Board
  - (U) High-level cyber S&T metrics

- **Evolving toward a Level 4 COI**
  - (U) International: Working multilateral cyber S&T agreements
  - (U) Academic: HBCU-MI Cyber Center of Excellence
  - (U) Industry: Engagement and collaboration leading to strategic Reliance
Outline

• BLUF
• Cyber COI Overview
• **Roadmap Development Process**
  • Cyber COI “4 + 2” S&T Roadmaps and Recent Successes
  • Hard Problems and Gaps
  • Engagements, Way Ahead, and Opportunities
• Summary
Cyber S&T Roadmap Evolution

2009 → 2010 → 2011 → 2012 → 2013 → 2014

- COI
- PSC
- COI

GOF Study 4.18
DoD S&T
Investment in
Cyberspace Security
and Information
Assurance

Cyber S&T
Capability
Framework

Way Ahead: CIMB &
Cyber Metrics Maturation

CIMB Driven Developments

Technology
Challenges

Cyber Forces Concept
of Employment

Roadmap
Development and
Priority Gaps
Cyber S&T Capability Framework

From CLMB Analysis of JS OV-5

**Defense**
- Reduce attack surface and increase resiliency of DODIN
- Reduce attack surface and increase resiliency of embedded/weapons systems
- Discover, understand, and engage threats

**Engagement**
- Active defense
- Respond to large-scale threats

**Situational Awareness and Courses of Action**
- Cyberspace situational awareness
- Understand cyber dependencies of missions
- Integrated course of action, cyber and non-cyber
Cyber S&T Capability Framework
Examples of High Level Metrics

Defense

• Increase total resources required by an adversary to achieve an effect
• Reduce adversary dwell time
• Reduce time until defense forces are aware of adversary

Engagement

• Increase cyber readiness
• Increase sophistication of campaign plans

Situational Awareness and Courses of Action

• Reduce time to map mission dependencies on cyber assets
• Improve robustness of mission-to-cyber mapping
• Increase quality of generated COA’s
Cyber S&T Roadmap
Technology Challenges & Cross Cutting Areas

Assuring Effective Missions
- Cyber Mission Control
- Scalable Operations

Agile Operations
- Cyber Maneuver
- Autonomic Cyber Agility

Resilient Infrastructure
- Resilient Architectures
- Resilient Algorithms and Protocols

Trust
- Trust Foundations

Embedded, Mobile, and Tactical (EMT)
## DoD's Joint Cyber S&T Focus Areas

<table>
<thead>
<tr>
<th>Focus Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Assuring Effective Missions</strong></td>
<td>Assess &amp; control the cyber situation in mission context</td>
</tr>
<tr>
<td><strong>Agile Operations</strong></td>
<td>Escape harm by dynamically reshaping cyber systems as conditions/goals change</td>
</tr>
<tr>
<td><strong>Resilient Infrastructure</strong></td>
<td>Withstand cyber attacks, while sustaining or recovering critical functions</td>
</tr>
<tr>
<td><strong>Trust</strong></td>
<td>Establish known degree of assurance that devices, networks, and cyber-dependent functions perform as expected, despite attack or error</td>
</tr>
<tr>
<td><strong>Embedded, Mobile, &amp; Tactical (EMT)</strong></td>
<td>Increase the capability of cyber systems that rely on technologies beyond wired networking and standard computing platforms</td>
</tr>
<tr>
<td><strong>Modeling, Simulation, &amp; Experimentation (MSE)</strong></td>
<td>Simulate the cyber environment in which the DoD operates to enable mission rehearsal and a more robust assessment and validation of cyber technology development</td>
</tr>
</tbody>
</table>
Outline

- BLUF
- Cyber COI Overview
- Roadmap Development Process
- **Cyber COI “4 + 2” S&T Roadmaps and Recent Successes**
- Hard Problems and Gaps
- Engagements, Way Ahead, and Opportunities
- Summary
Cyber FY15 S&T Across 4+2 Technology Areas

- **Funding Observations**
  - Appropriately increasing emphasis in AEM and EMT
  - Continued strong demand for Resilience
  - Trust focuses on military-unique topics
  - Agility operational goals and tradeoffs under discussion
  - Under-investment in MS&E resulting in acquisition and operational gaps

*Note: The EMT figures include some overlap with the other technology areas.*
Trust Foundations

Objectives / Accomplishments / Challenges

Objectives:
- Trusted Components and Architectures: Develop measures of trustworthiness for cyber components and large systems of varying pedigree and trustworthiness
- Scalable Supply Chain Analysis and Reverse Engineering: Analyze, attribute, and repurpose hardware and software at the speed and scale required for real-time strategic engagement

Accomplishments:
- FY13/14 Success Stories
  - Army: SW Assurance Toolkit (SWAT)
  - AF: Secure Processor
  - AF: Context/Content Aware Trusted Router
  - AF: Secure View

Technical Challenges:
- Development of Trust Anchors for component-level and composed HW and SW
- Tamper-proof/evident HW and SW components and systems
- Contextual threat/trust scoring calculus
- Rapid, assisted, and automated HW and SW analysis and validation
- Algorithms for accurate attribution of malware authors and supply chain tampering
# Trust Foundations Roadmap

<table>
<thead>
<tr>
<th>Area</th>
<th>FY13</th>
<th>FY14</th>
<th>FY15</th>
<th>FY16</th>
<th>FY17</th>
<th>FY18</th>
<th>FY19</th>
<th>FY20</th>
<th>FY21</th>
<th>FY22</th>
<th>FY23</th>
<th>FY24</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trusted Components and Architectures</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reduce DODIN attack surface and increase resiliency</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CSG</td>
<td>6</td>
<td>6</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SWAT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HACMS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trust Measurement and Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed Reputation Mgmt</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Context-Aware Trust Scoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Composite Trust Measures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vetting IT Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Active Defense</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack Surface Measurement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Define and Measure Surface</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System of Systems Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analyze trust mechanisms</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Scalable Supply Chain Analysis and Reverse Engineering</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto SW Vulnerability Discovery</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAPID</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manual RE/Assessment</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Detection of supply chain HW counterfeit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detection/mitigation of malicious HW functions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Key**
- **Funded**
- **Unfunded Gap**
- **DARPA**
- **Partially/Fully Unfunded Gap**
- **Expected TRL (#)**

*Distribution A – For Public Release*
Resilient Infrastructure
Objectives / Accomplishments / Challenges

Objectives:
- **Resilient Architectures**: Develop integrated architectures that are optimized for the ability to absorb shock and speed recovery to a known secure operable state.
- **Resilient Algorithms and Protocols**: Develop novel protocols and algorithms to increase the repertoire of resiliency mechanisms available to the architecture that are orthogonal to cyber threats.

Accomplishments:
- **FY13/14**
  - Army DEFIANT
  - Army: CRUSHPROOF

Technical Challenges:
- Assessment environments and tools for measuring resiliency of HW, SW, networks, and systems
- Calculus for relating resiliency concepts into measurable operational impact and automated DODIN defense actions
- Resilient overlay control planes that orchestrate defense of heterogeneous DODIN systems
- Secure, LPI/J, energy-efficient, mobile communication protocols
- Certifiable, agile, and affordable mobile device HW, OS, and app ecosystem
Resilient Infrastructure Roadmap

<table>
<thead>
<tr>
<th>FY13</th>
<th>FY14</th>
<th>FY15</th>
<th>FY16</th>
<th>FY17</th>
<th>FY18</th>
<th>FY19</th>
<th>FY20</th>
<th>FY21</th>
<th>FY22</th>
<th>FY23</th>
<th>FY24</th>
</tr>
</thead>
<tbody>
<tr>
<td>Near</td>
<td>Mid</td>
<td>Far</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resilient Architectures</td>
<td>Resiliency Metrics and Assessment</td>
<td>M&amp;S models for resiliency determination</td>
<td>In-situ resiliency analysis tools</td>
<td>Resilient Service Net</td>
<td>Threat-Aware Resilient Service Net</td>
<td>Resilient, Threat-Aware DODIN</td>
<td>Autonomous, self-managing resilient systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reduce Attack Surface/Increase Resiliency of the DODIN</td>
<td>JIE Hardened Cloud</td>
<td>Resilient Service Net</td>
<td>Threat-Aware Resilient Service Net</td>
<td>Resilient, Threat-Aware DODIN</td>
<td>Autonomous, self-managing resilient systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Control planes</td>
<td>Defiant</td>
<td>CRUSHPROOF</td>
<td>CND/IA</td>
<td>Control Planes for Heterogeneous Networks</td>
<td>Automated response and recovery</td>
<td>Resilient Frameworks</td>
<td>Autonomous Self-healing networks and hosts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Components &amp; Systems</td>
<td>Resilient multi-core processing</td>
<td>Threat-Aware System Resiliency</td>
<td>Resilient Frameworks</td>
<td>Autonomous Self-healing networks and hosts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Algorithms and Protocols</td>
<td>SW Resiliency</td>
<td>Resilience Validation Tools</td>
<td>Resilience Validation Tools</td>
<td>Resilience Validation Tools</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CRASH, SAFER</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Key:
- Yellow: Funded
- Gray: Unfunded Gap
- Purple: DARPA
- Red: Partially/Fully Unfunded Gap Expected TRL (#)

Distribution A - For Public Release
Agile Operations
Objectives / Accomplishments / Challenges

Objectives:
• **Cyber Maneuver**: Develop mechanisms that enable dynamically changing cyber assets to be marshaled and directed toward an objective – to create or maintain a defensive or offensive advantage.
• **Autonomic Cyber Agility**: Speed the ability to reconfigure, heal, optimize, and protect cyber mechanisms via automated sensing and control processes.

Accomplishments:
• Army: MorphiNator
• AF: ARCSYNE/COSYNE

Technical Challenges:
• Real-time, mission-aware traffic engineering including routing of threats
• Collaborative, coordinated cyber maneuver of multiple actors and forces (including coalition)
• Cyber maneuver for deceiving threats
• Dynamic reconfiguration of networks, systems and applications
• Autonomous reconfiguration
Agile Operations Roadmap

<table>
<thead>
<tr>
<th>Cyber Maneuver</th>
<th>Near</th>
<th>Mid</th>
<th>Far</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FY13</td>
<td>FY14</td>
<td>FY15</td>
</tr>
<tr>
<td><strong>Discover, understand, and engage Threats</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SAFER</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AIAC, Transparent Computing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Active Defense</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real-time, Mission-aware Traffic Engineering of Blue and Red</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real-time goal-based traffic engineering</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threat-based Dynamic Routing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Large Scale Threat Hardening</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DISN/624OC Transition</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Context Aware Decision Support</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mission/System Mapping and Modeling</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decision Support &amp; Commander's Intent</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workflow Analysis and Prediction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Respond to large-scale threats</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Autonomic real-time course of action management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MorphINator</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic reconfiguration and repurposing</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ambiguity Reasoning</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Graded and Automated Attack Mitigation Options</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARCS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Key:
- **Funded**
- **Unfunded Gap**
- **DARPA**
- Partially/Fully Unfunded Gap
- Expected TRL (#)

Distribution A – For Public Release
Assuring Effective Missions
Objectives / Accomplishments / Challenges

Objectives:
- Cyber Mission Control: Develop tools and techniques that enable efficient models of cyber operational behaviors (cyber and kinetic) to determine the correct course of action in the cyber domain
- Scalable Operations: Develop ability to operate and survive during operations conducted by large-scale threats

Accomplishments:
- Promised last year for FY13
  - OSD: Purple Musket
  - Navy: Flying Squirrel BT Integration
- FY13/14 AF: Mission Aware Cyber C2 (MACC2)

Technical Challenges:
- Tools for mapping and real-time analysis of missions to enable cyber/kinetic situational awareness
- Understanding dynamically evolving missions and their dependencies, identifying cyber/kinetic change indicators, updating models and resolving cross-dependencies, projecting change trends
- Decision Support and reasoning tools that factor in multiple dimensions (e.g., attribution, severity, reversibility of effect, BDA, ...)

Cyber Col
14-Nov-14 Page-23

Distribution A – For Public Release
## Modeling, Simulation, & Experimentation

### Objectives / Accomplishments / Challenges

#### Objectives:
- **Simulation and Experimentation Technology:**
  - Enable robust, quantifiable, and repeatable assessment and validation of candidate cyber technology
- **Models & Analysis:**
  - Simulate the cyber operational environment with high fidelity
  - Describe and predict interactions and effect between physical and cyber domains

#### Accomplishments:
- Sequoia HPC achieved world record $10^{15}$ events/sec
- Army: Cyber Army Modeling & Simulation (CyAMS)
- AF: Cyber Experimentation Environment

#### Technical Challenges:
- Automated, rapid instantiation of large-scale, complex computing and network environments
- Objective architecture for heterogeneous range component integration and synchronization
- M&S for large-scale aggregate Internet behavior, operating at multiple timescales
- Integrated high-fidelity models of kinetic and cyber phenomena
- Human behavioral and intention models
- Planning and Assessment algorithms to evaluate operational agility and assurance
# Modeling, Simulation, and Experimentation (MSE) Roadmap

**Simulation & Experimentation Technology**

<table>
<thead>
<tr>
<th></th>
<th>Near FY13</th>
<th>FY14</th>
<th>FY15</th>
<th>FY16</th>
<th>FY17</th>
<th>FY18</th>
<th>FY19</th>
<th>FY20</th>
<th>FY21</th>
<th>FY22</th>
<th>FY23</th>
<th>FY24</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respond to Large-scale Threats</td>
<td>NCR</td>
<td>CEE</td>
<td>CyAMS</td>
<td>NCR</td>
<td></td>
<td>Joint IO Range Architecture Upgrade</td>
<td>Joint IO Range Fidelity/Scale Upgrade</td>
<td>Automated instantiation of large-scale complex network environments</td>
<td>Objective Architecture for Cyber Experiment and Test</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M &amp; S for large-scale aggregate behavior, operating at multiple timescales</td>
<td>Sequoia PDES @ 10^15</td>
<td>Validated Cyber Benchmark</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Country-Level Simulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Models & Analysis**

<table>
<thead>
<tr>
<th></th>
<th>FY13</th>
<th>FY14</th>
<th>FY15</th>
<th>FY16</th>
<th>FY17</th>
<th>FY18</th>
<th>FY19</th>
<th>FY20</th>
<th>FY21</th>
<th>FY22</th>
<th>FY23</th>
<th>FY24</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understand Cyber Dependencies of Missions // Integrated COA // Discover, Understand, Engage Threats</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Cyber Ops Plan/Assess Tool</td>
<td>Cyber-Kinetic Planning/Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrated high-fidelity models of kinetic and cyber phenomena</td>
<td>Large Scale Cyber Quantification</td>
<td>Internodal Modeling</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Human behavioral and intent models</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Key**

- Funded
- Unfunded Gap
- DARPA
- Partially/Fully Unfunded Gap
- Expected TRL (#)
### Objectives:

- **Mobile and Tactical Systems Security**
  - Secure information sharing at tactical edge
  - Reduction of mobile computing attack surface in all its aspects

- **Embedded Tactical Composite Trust**
  - Architectural approaches for composing embedded systems
  - Security capabilities needed for robust and secure composed systems

- **Leverage International Partners**

### Accomplishments:

- **Navy:** Network Pump – II

- **Army:** Tactical Army Cross Domain Information Sharing (TACDIS)

### Technical Challenges:

- Secure, LPI/J, energy-efficient, mobile communication protocols
- Certifiable, agile, and affordable mobile device hardware, OS, and app ecosystem
- Tools to monitor and assess assurance of cyber operations in converged strategic/tactical systems
- Self-monitoring systems in systems, including real-time integrity measurement
- Tools to monitor and assess the health and behaviors of embedded cyber systems - security of weapons systems and platforms

---

Apply the Cyber S&T Roadmap to Embedded, Mobile, and Tactical Environments
## Embedded, Mobile and Tactical Roadmap

<table>
<thead>
<tr>
<th></th>
<th>FY13</th>
<th>FY14</th>
<th>FY15</th>
<th>FY16</th>
<th>FY17</th>
<th>FY18</th>
<th>FY19</th>
<th>FY20</th>
<th>FY21</th>
<th>FY22</th>
<th>FY23</th>
<th>FY24</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Near</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile and</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tactical</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cyberspace</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Situational</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Awareness</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mid</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Assurance</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>of Converged</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile &amp;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Back-end</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Reduce</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack Surface</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&amp; Increase</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resiliency of</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Embedded/Tac</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>tical Systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Far</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Secure</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Embedded</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Architectures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Distribution</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A—For Public</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Release</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Key
- **Funded**
- **Unfunded Gap**
- **DARPA**
- **Partially/Fully Unfunded Gap**
- **Expected TRL (#)**
Outline

• BLUF
• Cyber COI Overview
• Roadmap Development Process
• Cyber COI “4 + 2” S&T Roadmaps and Recent Successes
• Hard Problems and Gaps
  • Engagements, Way Ahead, and Opportunities
• Summary
Specific Gap Assessment

Defense
- Trustworthy embedded system architectures composed of components of mixed trust
- Trust scoring mechanisms
- Scalable HW/SW analysis and verification techniques
- Resilient mobility

Engagement
- Control planes for heterogeneous components and systems
- Threat-aware defenses
- Real-time defensive traffic management

Situational Awareness and Courses of Action
- Graded options responsive to commander’s intent
- Analysis of Mission Dependencies to Cyber Infrastructure
- Cyber-Kinetic integration, planning, and assessment

Measurement and Metrics
- Quantifiable attack surface measurement
- Component and system resiliency metrics
- Threat-based agility metrics
- Calculus for Mission Assurance
- Cyber modeling and simulation and experimentation
Outline

• BLUF
• Cyber COI Overview
• Roadmap Development Process
• Cyber COI “4 + 2” S&T Roadmaps and Recent Successes
• Hard Problems and Gaps
• Engagements, Way Ahead, and Opportunities
• Summary
Community Engagement

- TTCP Cyber Grand Challenge (Kickoff Jun 2014)
  - Trust Foundations
  - Mission Assurance Through Mission Awareness (MASA)
  - Integrated Cyber-EW Operations

- STRATCOM/J8 EW-Cyber ICD (Draft Dec 2014)

- Five RDA-TFs for Cyber

- DoD Innovation Marketplace
  - Bi-Weekly engagement
  - AFRL IR&D Review
DoD Unique Cyber Capabilities

- **Experimentation/Assessment**
  - Cyber Experimentation Environment (CEE)
  - Army Cyber Research & Analytics Laboratory (ACAL)
  - D-Shell
  - High Performance Computing (HPC)
  - CND data sets

- **Ranges**
  - National Cyber Range (NCR)
  - Joint IO Range (JIOR)

- **Maturing Capabilities**
  - Contested Cyber Environment (CCE)
  - Network Integration Environment (NIE)

- **Telecommunications/Wireless**
  - Telecommunications Labs (CERDEC)
  - Communications System Integration Laboratory (CSIL)
  - HI-FI Advance Waveform and Cyber laboratory
  - Electromagnetic Environment (EME)
DoD Cyber Transition to Practice (CTP) Initiative

Emerging "Best of Breed" S&T Matured through Cyber Range-based T&E, Demonstrations, and Operational Pilots

- CTP is maturing and transitioning DoD-funded cyber S&T
  - Get S&T addressing key gaps into Ops
  - White House priority
  - Increase TRL, reduce risk
- CTP emphasizes:
  - Rapid results near term
  - Committed transition partner(s)
  - Co-funding by transition partner(s)

- FY14 funding: $4.2M
- Two white paper rounds so far
  - Phase 1: DoD Labs, DARPA, NSA
  - Phase 2: UARCs, FFRDCs, SPAWAR
- 8 projects underway
- Future
  - Planning currently underway for next phase of CTP
Industry Engagement - Way Ahead

- **Strategic DoD-Industrial cooperation in security marketplace**
  - Metrics development
  - Standards bodies participation/voting
  - Army: Cooperative development model with industry
  - Intellectual Property business cases that reduce market friction

- **DoD-Industrial Collaboration and Co-Development**
  - Personnel Exchanges
  - Cooperative R&D Agreements (CRADA)
  - Experimentation, T&E Ranges

- **Increase speed of cyber acquisition**
  - Enhanced M&S for early assessment of S&T candidates
  - Rapid-response S&T development
    - Examples: DARPA Cyber Fast Track, AFRL ACT IDIQ...other Services also exploring similar vehicles

- **OTHER IDEAS?**
Defense Innovation Marketplace
Resources For Industry And DoD

CONNECTING INDUSTRY & DoD
The Defense Innovation Marketplace is a centralized resource to reinvigorate innovation.
For Industry: the Marketplace is a resource for information about Department of Defense (DoD) investment priorities and capability needs.
For Government: the Marketplace provides access to search tools to assess and then leverage industry R&D projects for current and future programs.

Marketplace: Resources for DoD
- Secure portal with 10,000+ IR&D Project Summaries
- Access for DoD S&T/ R&D and Acquisition Professionals
- DoD Searchers encouraged to contact the Industry POC listed on project summaries of interest

Marketplace: Resources for Industry
- DoD R&D Roadmaps; Investment Strategy
- Business Opportunities with the DoD
- Virtual Interchanges & Events
- Secure Portal for IR&D Project Summaries
- Top Downloads/Pages visited
- DoD IR&D SEARCH Trends

Additional Resources

- **DIA Needipedia** (http://www.dia.mil/Business/Needipedia.aspx)
  - Provides a direct channel of Defense Intelligence Agency (DIA) needs into the emerging technology community

- **FedBizOps** (https://www.fbo.gov/)
  - Portal into government acquisitions providing a centralized repository for federal contract opportunities.

- **SBIR Announcements** (http://www.dodsbir.net)
  - Resource center for DoD SBIR

- For more information on DoD cyber Science & Technology news, research needs and engagement opportunities, visit:
  - Army Research Office (ARO)/Army Research Lab (ARL) (http://www.arl.army.mil)
  - Office of Naval Research (ONR) (http://www.onr.navy.mil)
  - Naval Research Laboratory (NRL) (http://www.nrl.navy.mil)
  - Defense Advanced Research Projects Agency (DARPA) (http://www.darpa.mil)
Contacts

- **OSD SG Rep: Dr Steven King**
  - OSD SG Rep
  - OASD(R&E) Deputy Director Cyber Technologies
  - (571) 372-6710
  - Steven.E.King.50.civ@mail.mil

- **Army SG Rep: Mr. Henry Muller**
  - CERDEC Acting Director
  - POC: Mr. Giorgio Bertoli
  - (443) 861-0743
  - Giorgio.Bertoli.civ@mail.mil

- **Navy SG Rep: Dr. Wen Masters**
  - Office of Naval Research
  - POC: Dr. Gary Toth
  - (703) 696-4961
  - Gary.Toth@navy.mil

- **NSA SG Rep: Dr. Boyd Livingston**
  - NSA/R Chief Scientist for Research
  - POC: Dr. Grant Wagner
  - (443) 634-4200
  - gmw@tycho.nsa.mil

- **SG Lead: Dr Richard W. Linderman**
  - Cyber COI Steering Group Chair
  - AFRL/RI Chief Scientist
  - (315) 330-4512
  - Richard.Linderman@us.af.mil

- **WG Lead: Mr. Chester Maciag**
  - Cyber COI WG Chair
  - AFRL/RI Principal Cyber S&T Strategist
  - (315) 330-2560
  - Chester.Maciag@us.af.mil
Summary

- Established, mature, and coordinated community
- Cyber S&T aligned to expanding operational capability gaps/priorities
- Cyber S&T contributions to nearly all Seven DoD Hard Problems
- Driving deeper engagement with industry and international partners
BACKUP
DoD Cyber Ecosystem

Large Defense Contractors
Small Businesses
System Integrators
Trusted Hardware/Software Manufacturing
Information Technology Vendors
Venture Capitalists
Non-traditional Defense Companies

Business Systems
Data Systems
High Performance Computing Systems
IT Systems
Weapon Systems
Many More...

DOD CUSTOMERS

ACADEMIA

DOD LABS

GOOD IDEAS

DOD PROGRAMS