The overall classification of this briefing is
UNCLASSIFIED

NDIA Hard Problems Workshop - Cyber COI Deep Dive

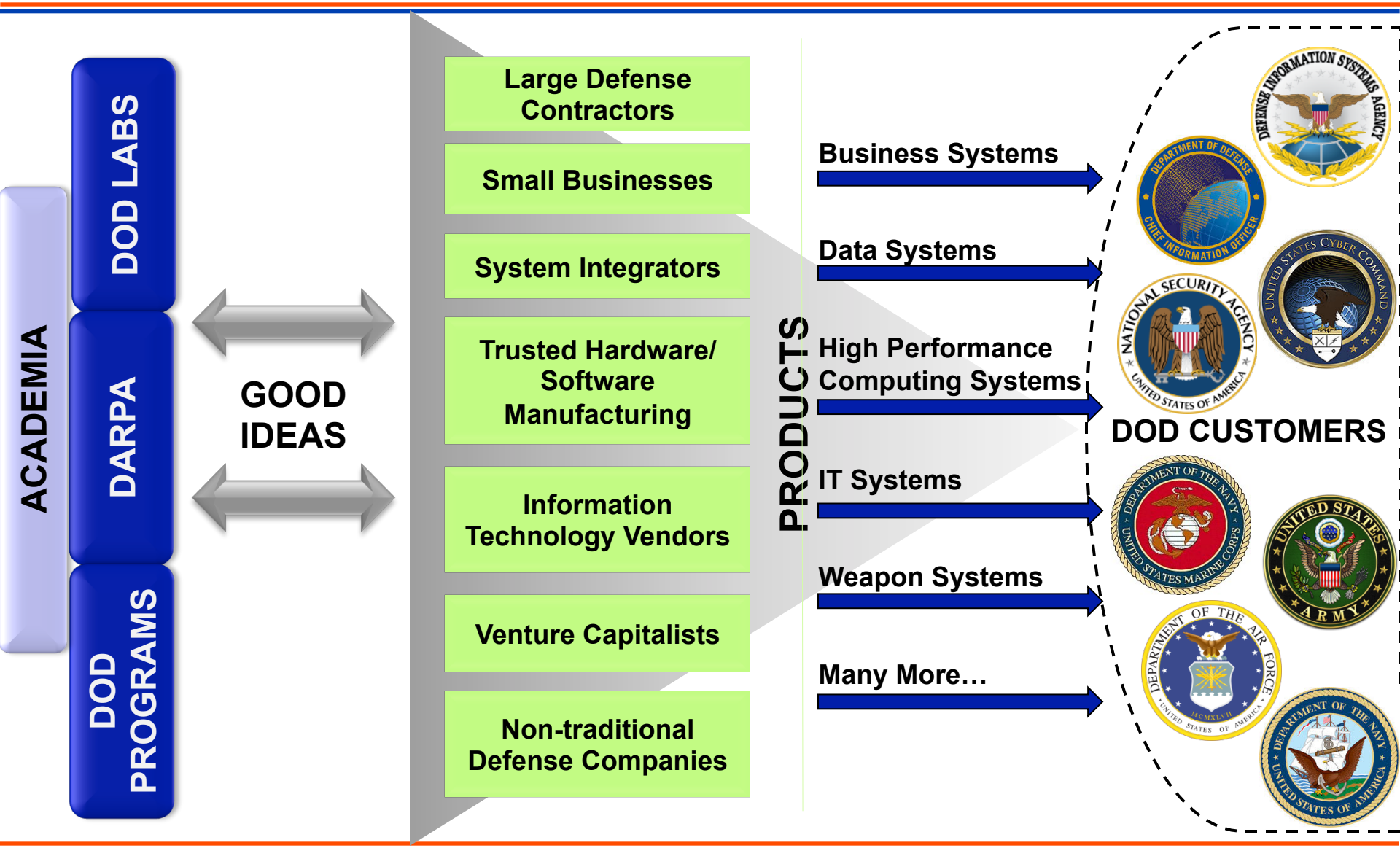
5 Nov 14

Dr. Richard Linderman

Cyber COI Steering Group Lead

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

DoD Cyber Ecosystem



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

Cyber Investment Management Board (CIMB)

COCOMs

Department of Defense Strategy for Operating in Cyberspace

CYBERSPACE POLICY REVIEW

TRUSTWORTHY CYBERSPACE: STRATEGIC PLAN FOR THE FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAM

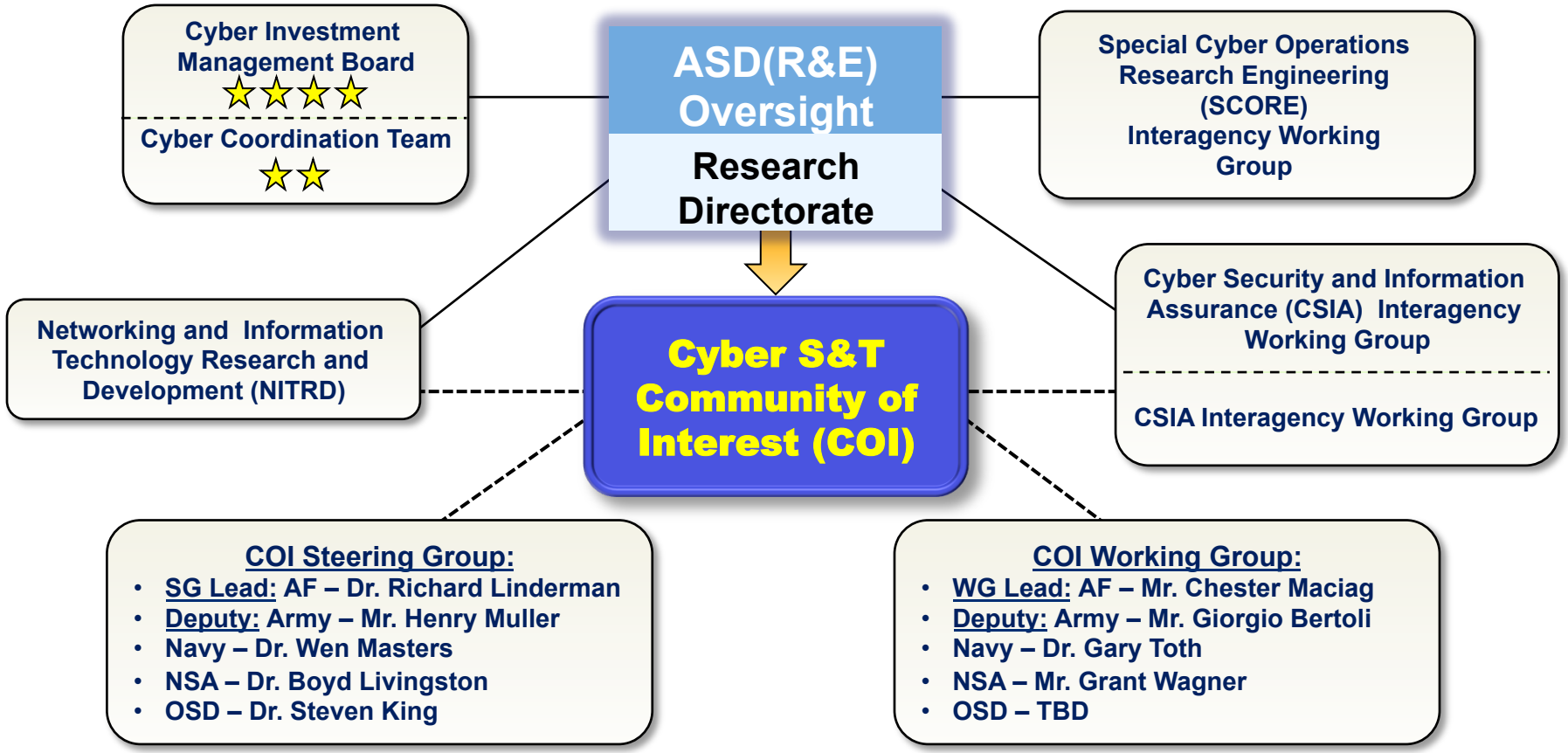
S&T Community of Interest

Enhance United States National Security & Economic Prosperity

- Defend the Homeland
- Build Security Globally
- Project Power and Win Decisively

Mission Assurance
Agility
Resiliency
Foundations of Trust

DoD Cyber S&T Coordination



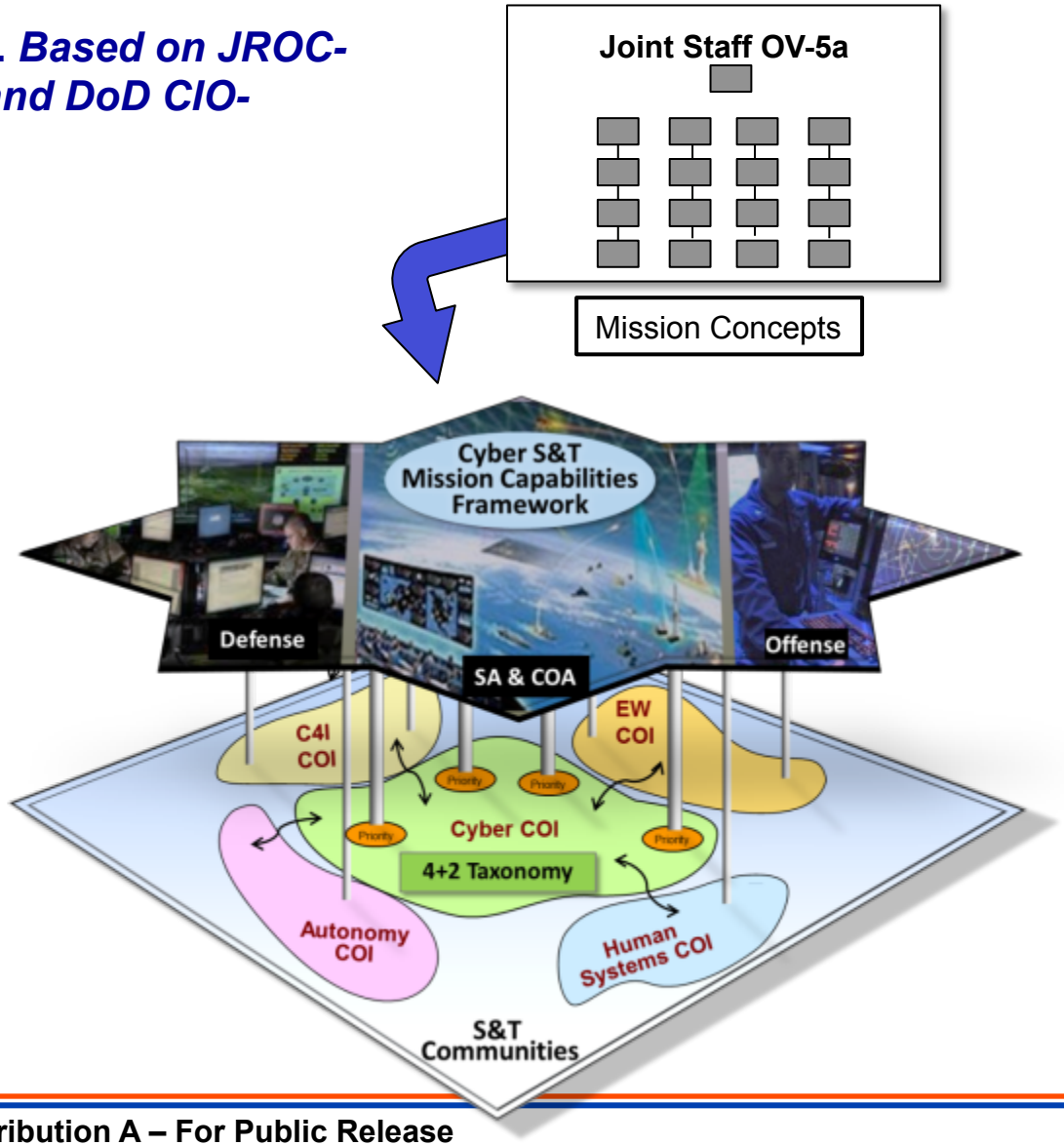
Users			Research Community					Users		
DISA	NSA IAD	DCIO	ONR/ NRL	AFRL/ AFOSR	NSA Research	DARPA	RDECOM	DTRA	USSTRATCOM/ USCYBERCOM	USD(I)

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

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

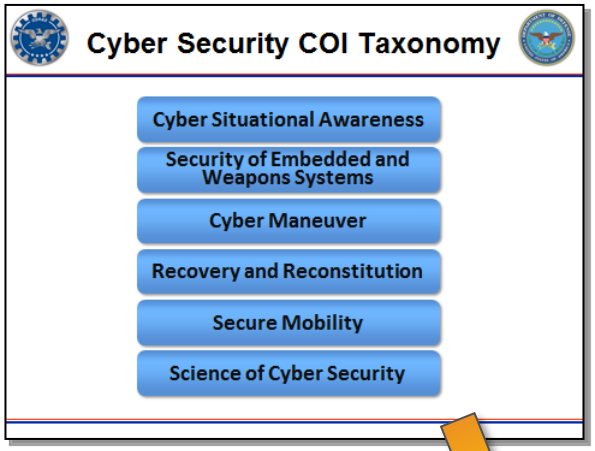


Cyber COI Recent Activities

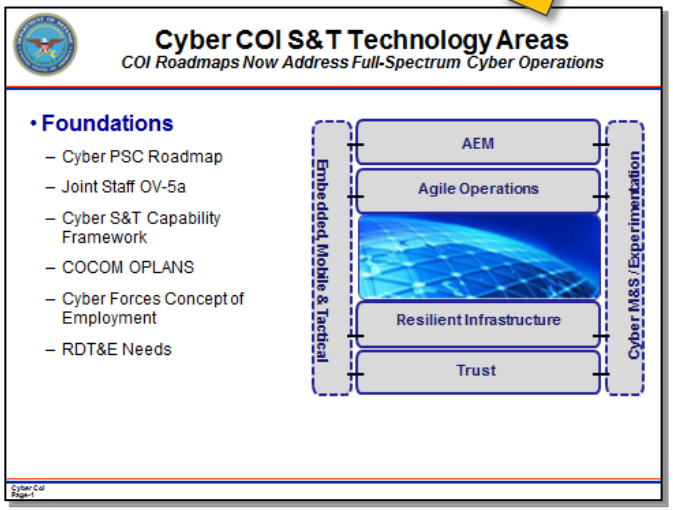
- **Briefed roadmap to S&T EXCOM in May**
  - Cyber PSC → Cyber [Security] COI
  - Incorporated findings of Cyber Investment Management Board
  - High-level cyber S&T metrics

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

Circa 2009



TODAY



Cyber S&T Capability Framework

From CIMB 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

Modeling, Simulation, and Experimentation (MSE)

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

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

CROSS CUTTING

Specific Gap Assessment

Defense

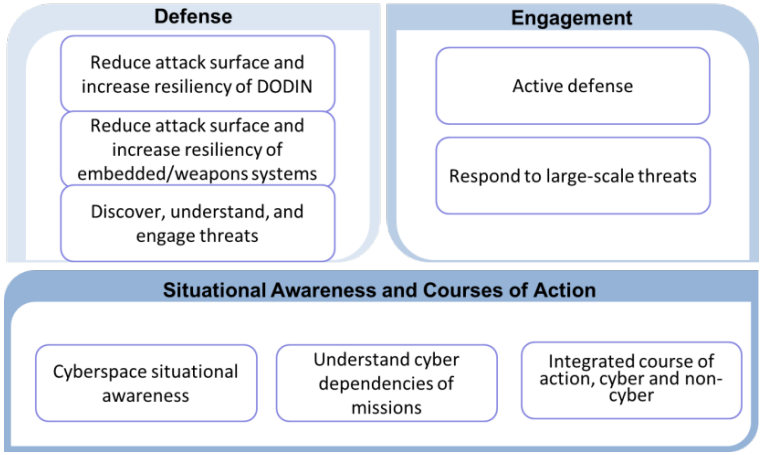
- Trustworthy embedded system architectures composed of components of mixed trust
- Trust scoring mechanisms
- Scalable HW/SW analysis and verification techniques
- Resilient mobility

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



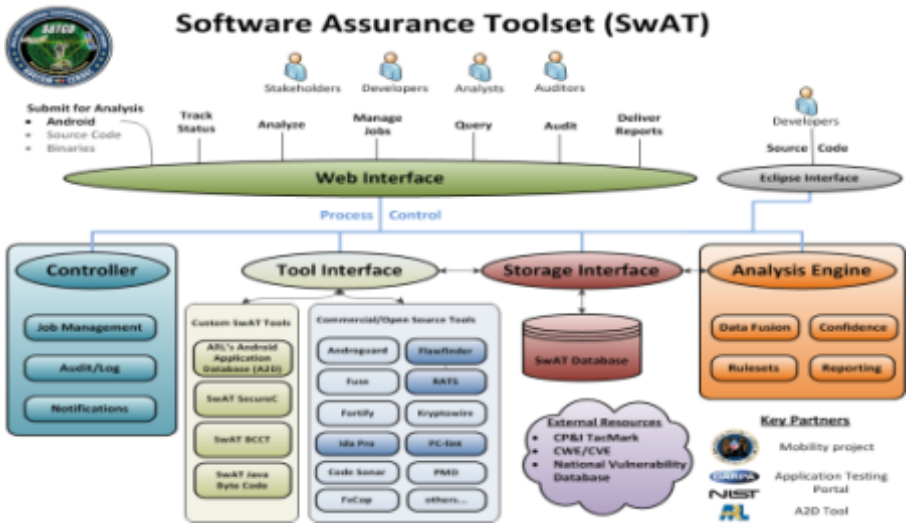
Measurement and Metrics

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

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:

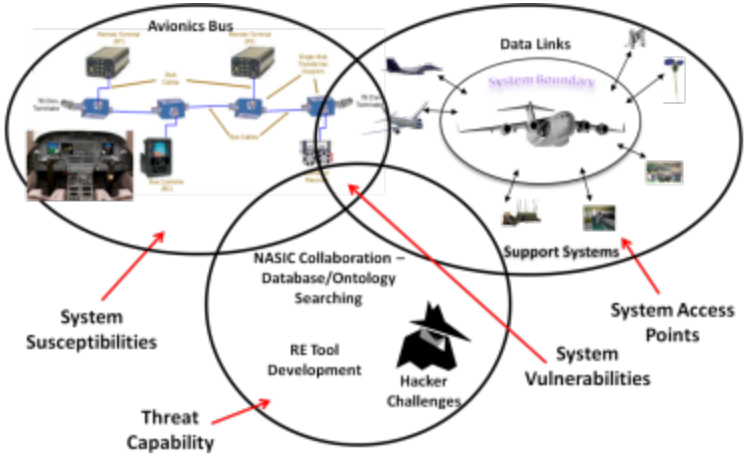
- Development of Trust Anchors for component-level and composed HW and SW
- Tamper-proof/evident HW and SW components and systems
- Contextual threat/trust scoring calculus
- Rapid, assisted, and automated HW and SW analysis and validation
- Algorithms for accurate attribution of malware authors and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

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

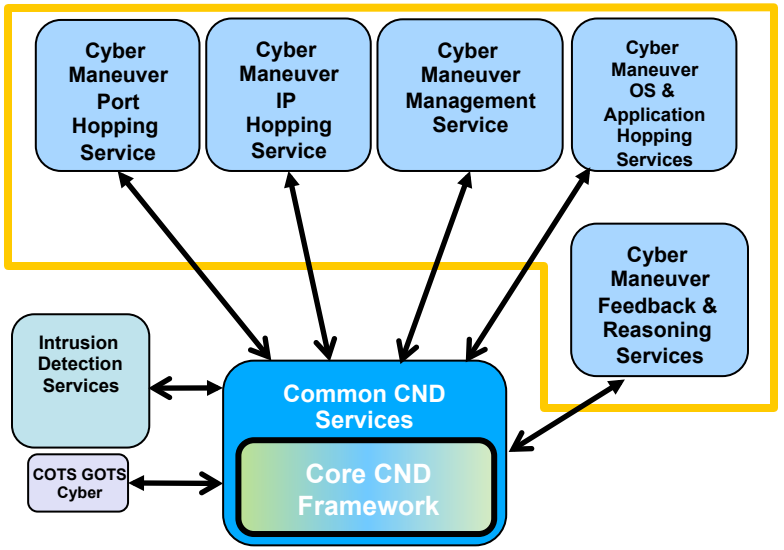
Technical Challenges:

- 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

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

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:

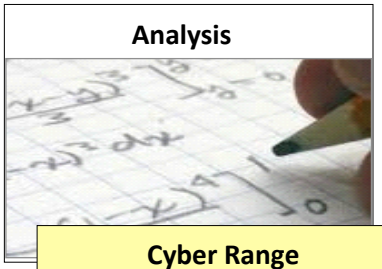
- Tools for mapping and real-time analysis of missions to enable cyber/kinetic situational awareness
- Understanding dynamically evolving missions and their dependencies, identifying cyber/kinetic change indicators, updating models and resolving cross-dependencies, projecting change trends
- Decision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

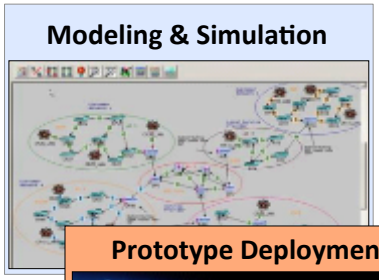
Modeling, Simulation, & Experimentation

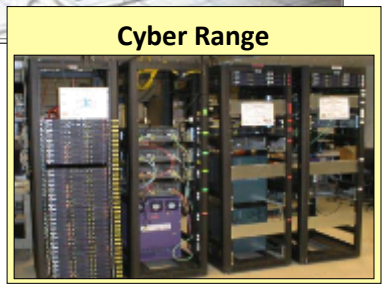
Objectives / Accomplishments / Challenges

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

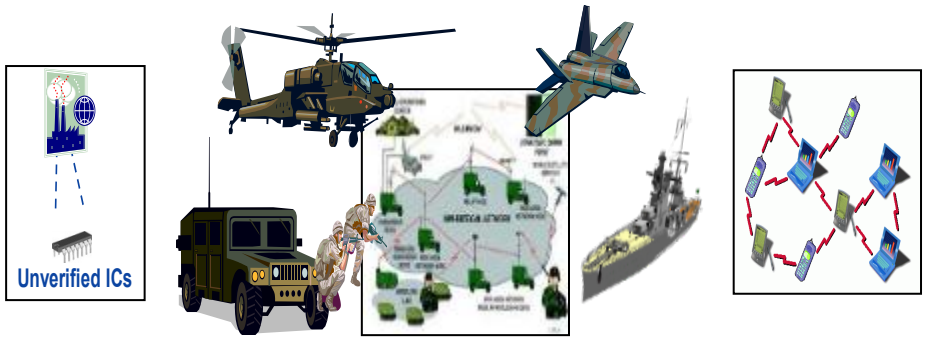
Technical Challenges:

- 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

Embedded, Mobile, and Tactical
Objectives / Accomplishments / Challenges

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**



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

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