Report Documentation Page		*Form Approved* *OMB No. 0704-0188*
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.		

1. REPORT DATE **NOV 2014**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **NDIA Hard Problems Workshop Cyber COl Deep Dive (U)**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **AFRL/RI, 525 Brooks Rd, Rome NY 13441-4505**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT **Approved for public release, distribution unlimited**

13. SUPPLEMENTARY NOTES **The original document contains color images.**

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT **SAR**	18. NUMBER OF PAGES **41**	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**			

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

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**
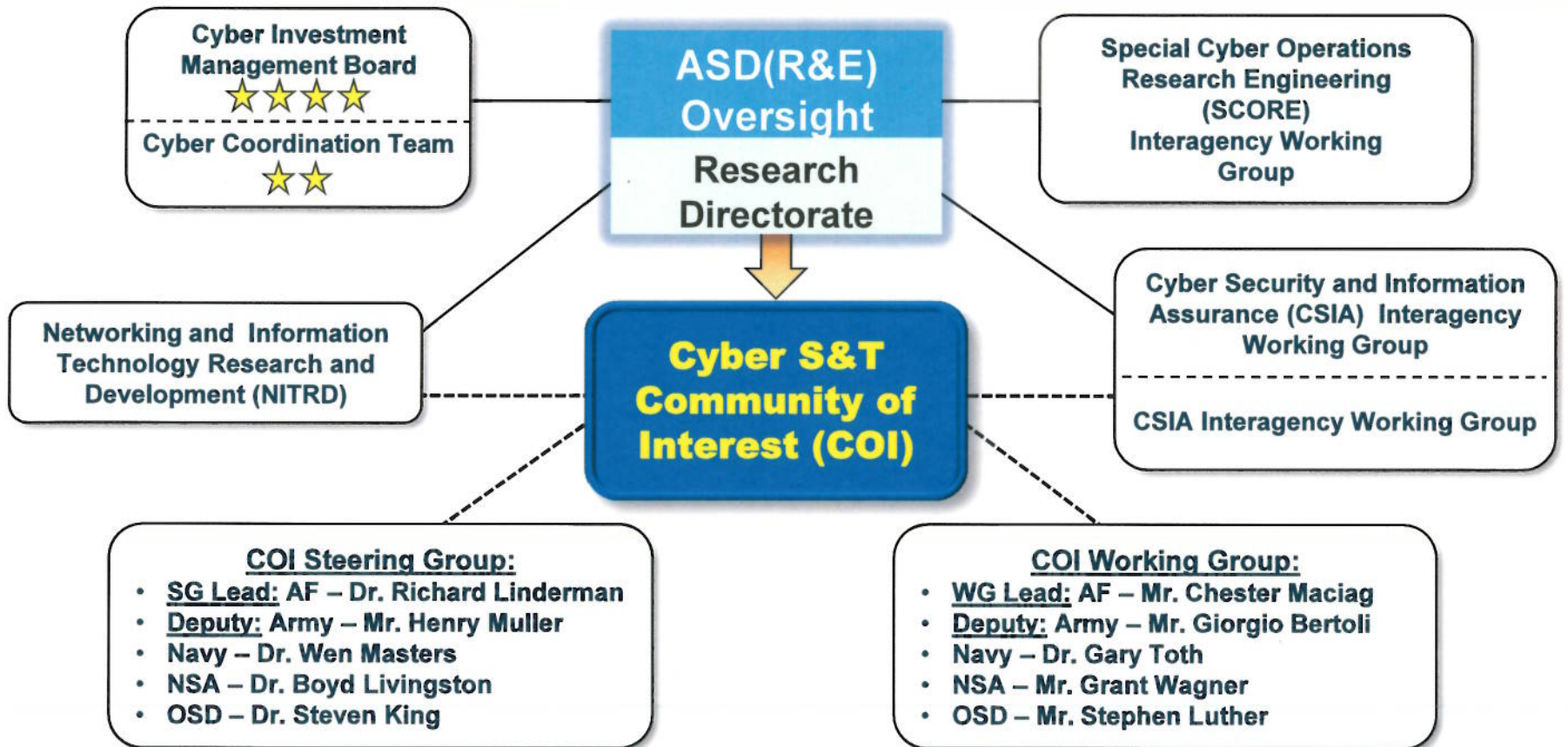
S&T Influencing the DoD Cyber Landscape

"…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

Cyber Investment Management Board (CIMB)

COCOMs

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

Cyber Investment Management Board
★★★★

- - -

Cyber Coordination Team
★★

ASD(R&E) Oversight

Research Directorate

Special Cyber Operations Research Engineering (SCORE) Interagency Working Group

Networking and Information Technology Research and Development (NITRD)

Cyber S&T Community of Interest (COI)

Cyber Security and Information Assurance (CSIA) Interagency Working Group

- - -

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	Research Community	Users

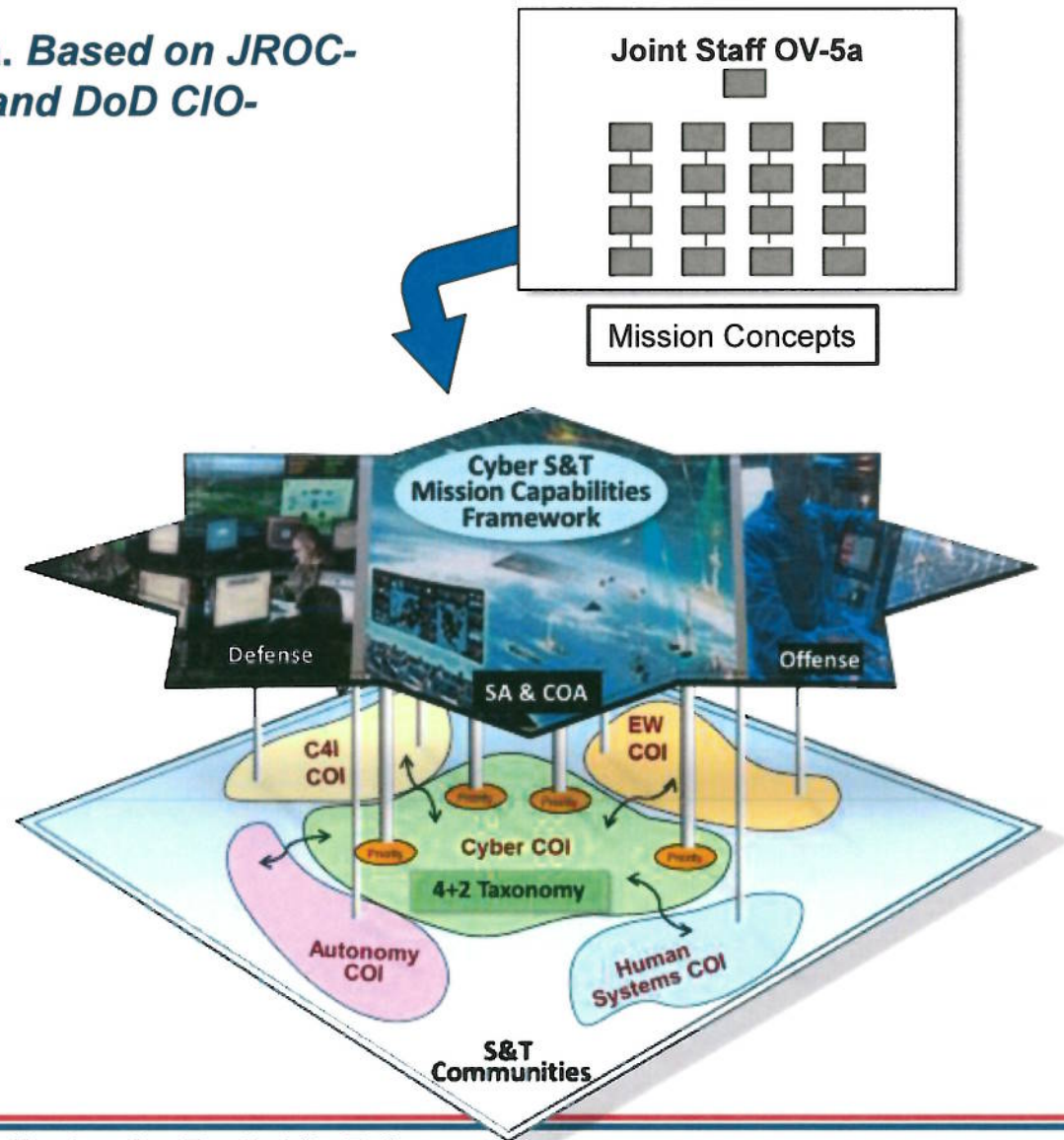| DISA	NSA IAD	DCIO	ONR/ NRL	AFRL/ AFOSR	NSA Research	DARPA	RDECOM	DTRA	USSTRATCOM/ USCYBERCOM	USD(I)

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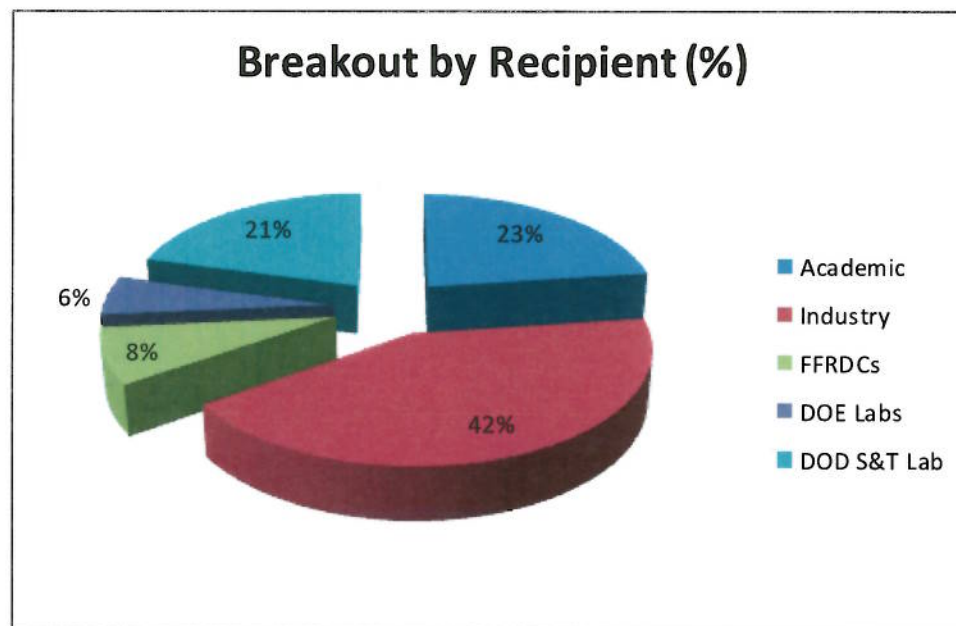
- Spans Defense, Effects, Situational Awareness-Course of Action
- Includes enterprise, tactical and embedded
- Cuts across all domains
- Touches C4I, EW, Autonomy, and Human Systems COIs
- Transcends S&T across all DOTMLPF
- QDR Tenets Addressed
  - Mitigates Threats
  - Delivers Affordable Capability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

Joint Staff OV-5a

Mission Concepts

Cyber S&T Mission Capabilities Framework

Defense

Offense

SA & COA

C4I COI

EW COI

Cyber COI

4+2 Taxonomy

Autonomy COI

Human Systems COI

S&T Communities

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
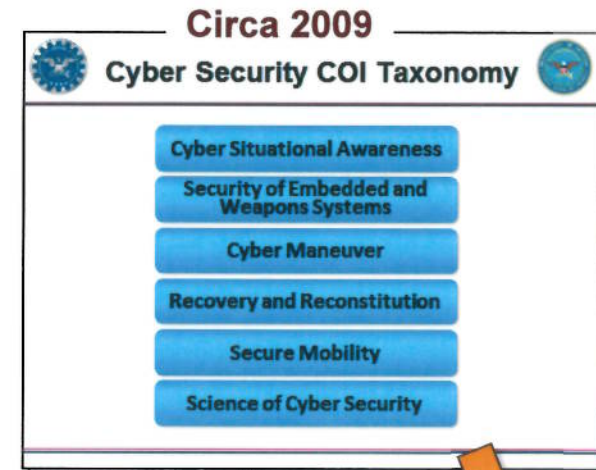- DOE Labs
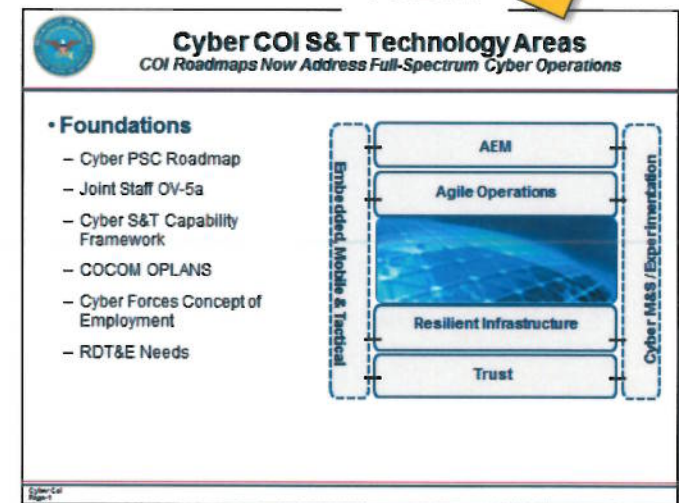- DOD S&T Lab

23% — 42% — 8% — 6% — 21%

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

Circa 2009

Cyber Security COI Taxonomy

- Cyber Situational Awareness
- Security of Embedded and Weapons Systems
- Cyber Maneuver
- Recovery and Reconstitution
- Secure Mobility
- Science of Cyber Security

TODAY

Cyber COI S&T Technology Areas
COI Roadmaps Now Address Full-Spectrum Cyber Operations

- **Foundations**
  - Cyber PSC Roadmap
  - Joint Staff OV-5a
  - Cyber S&T Capability Framework
  - COCOM OPLANS
  - Cyber Forces Concept of Employment
  - RDT&E Needs

  - AEM
  - Agile Operations
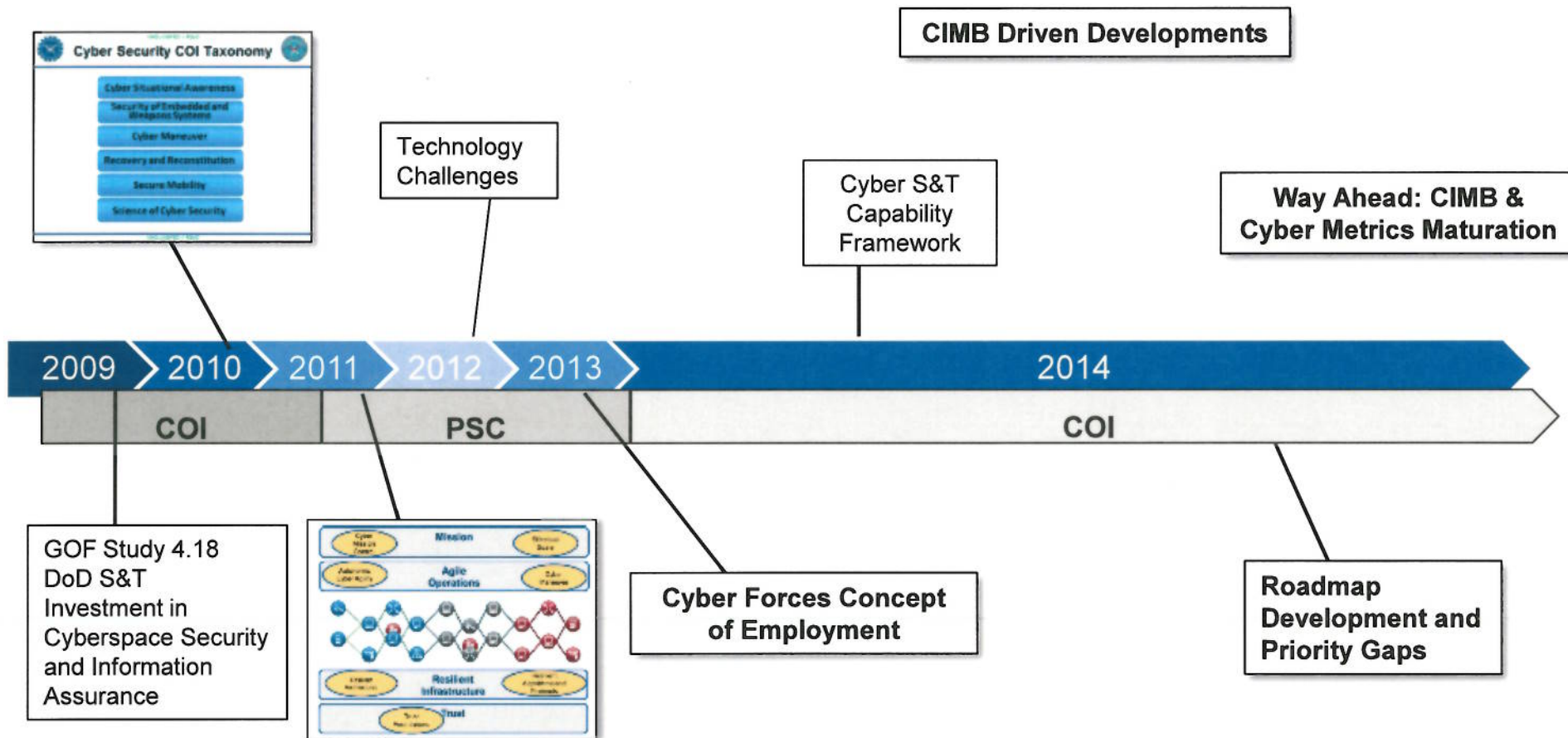 - Resilient Infrastructure
  - Trust

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

CIMB Driven Developments

Cyber Security COI Taxonomy
- Cyber Situational Awareness
- Security of Embedded and Weapons Systems
- Cyber Maneuver
- Recovery and Reconstitution
- Secure Mobility
- Science of Cyber Security

Technology Challenges

Cyber S&T Capability Framework

Way Ahead: CIMB & Cyber Metrics Maturation

2009	2010	2011	2012	2013	2014
COI		PSC			COI

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

Cyber Forces Concept of Employment

Roadmap Development and Priority Gaps

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
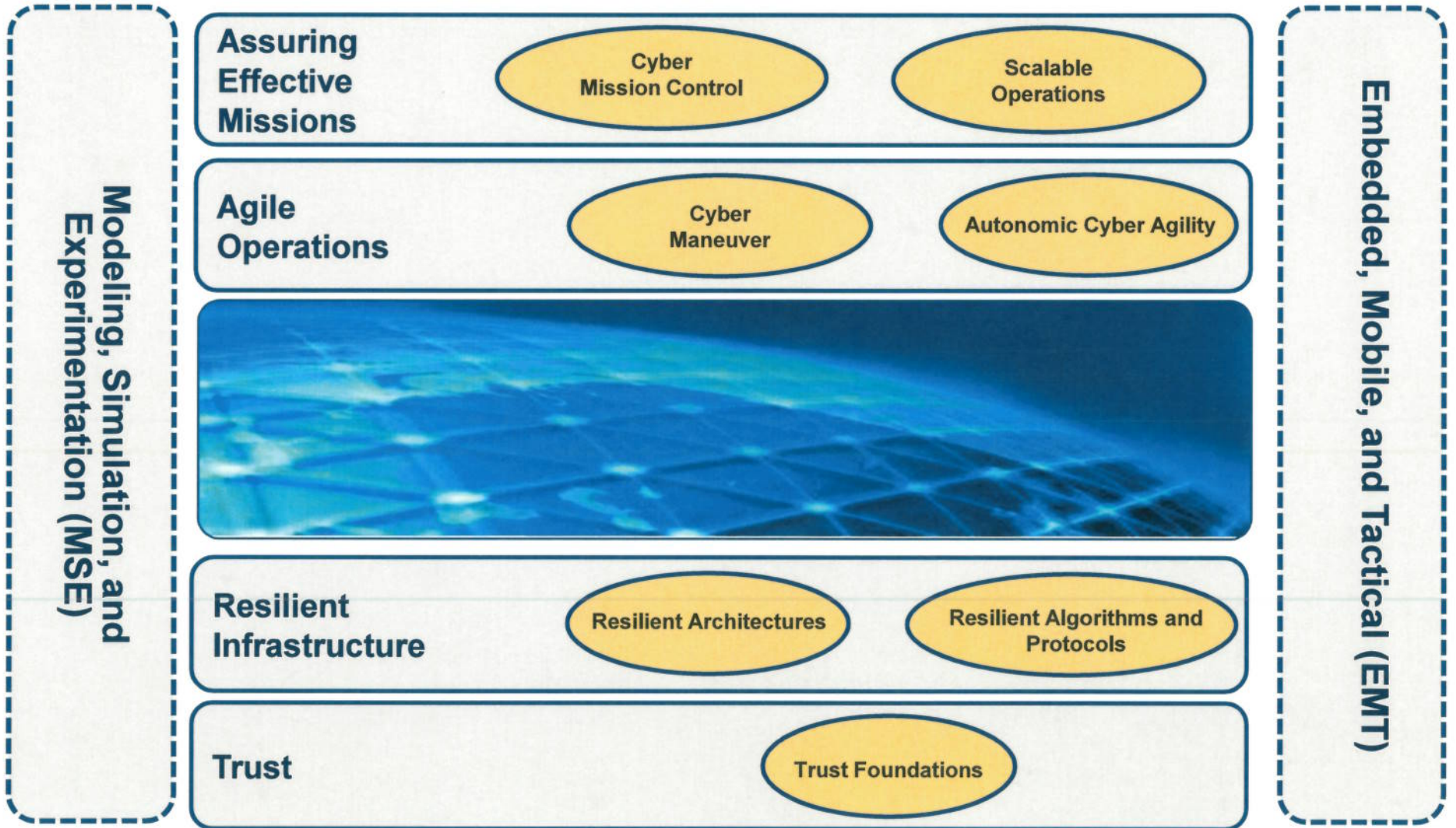- Increase sophistication of campaign plans

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)

Embedded, Mobile, and Tactical (EMT)

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

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
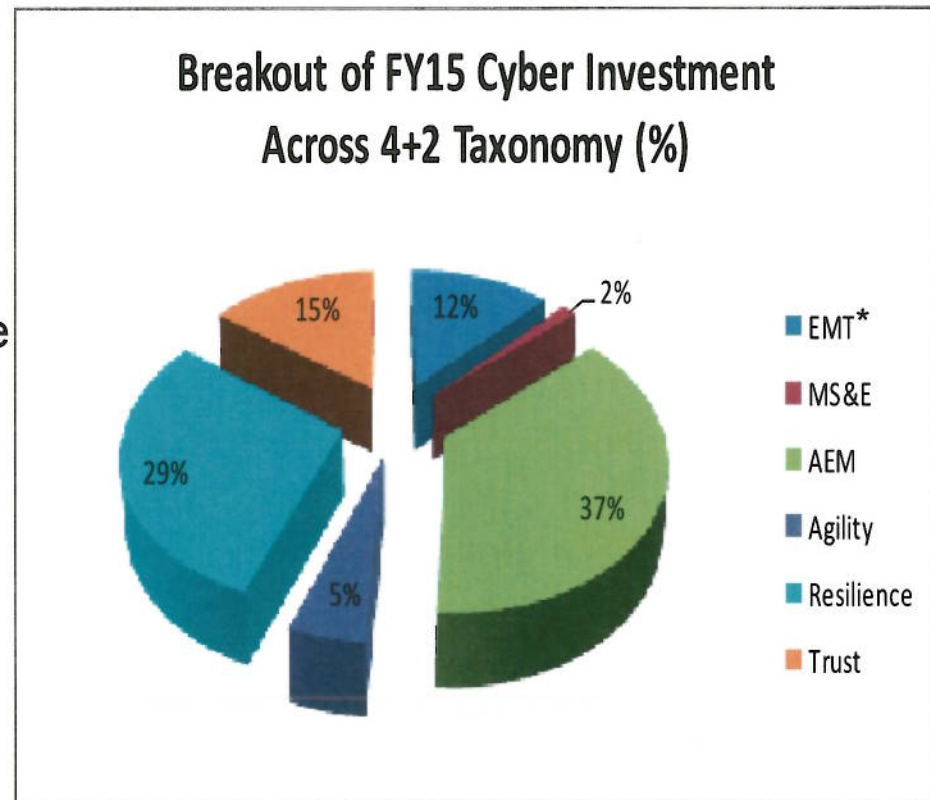
CROSS CUTTING

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

- **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

Breakout of FY15 Cyber Investment Across 4+2 Taxonomy (%)

- EMT*
- MS&E
- AEM
- Agility
- Resilience
- Trust

15% 12% 2% 29% 5% 37%

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

Trust Foundations
Objectives / Accomplishments / Challenges

Software Assurance Toolset (SwAT)

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
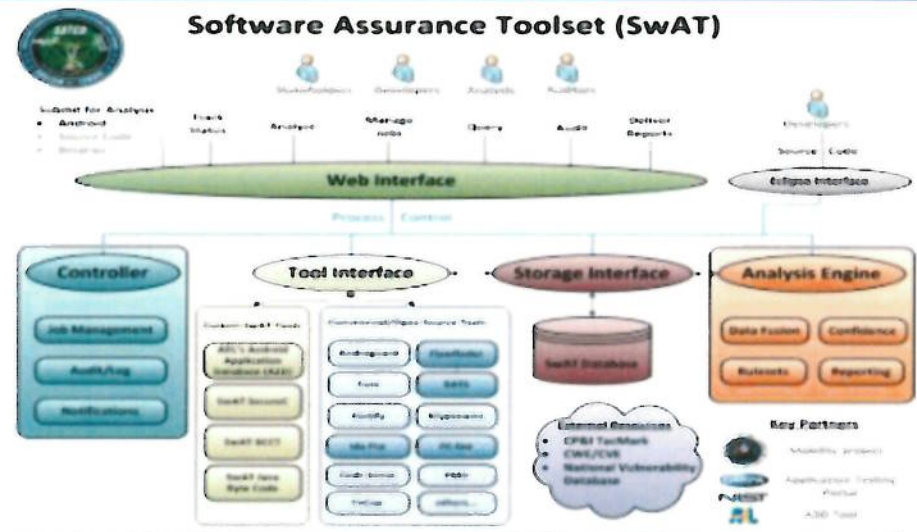
Accomplishments:

- 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

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.
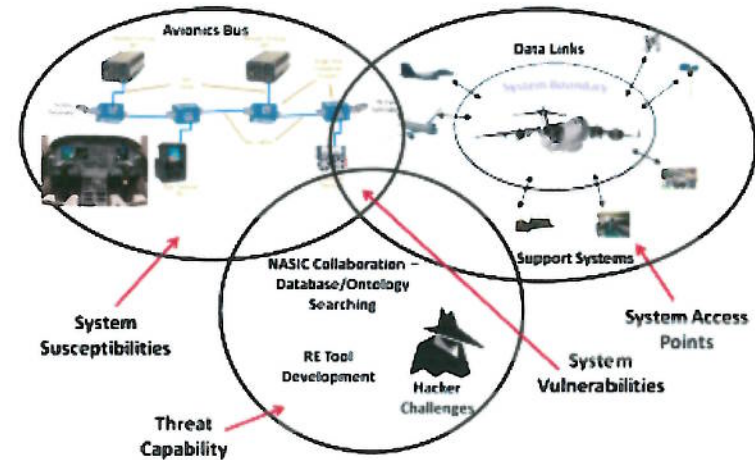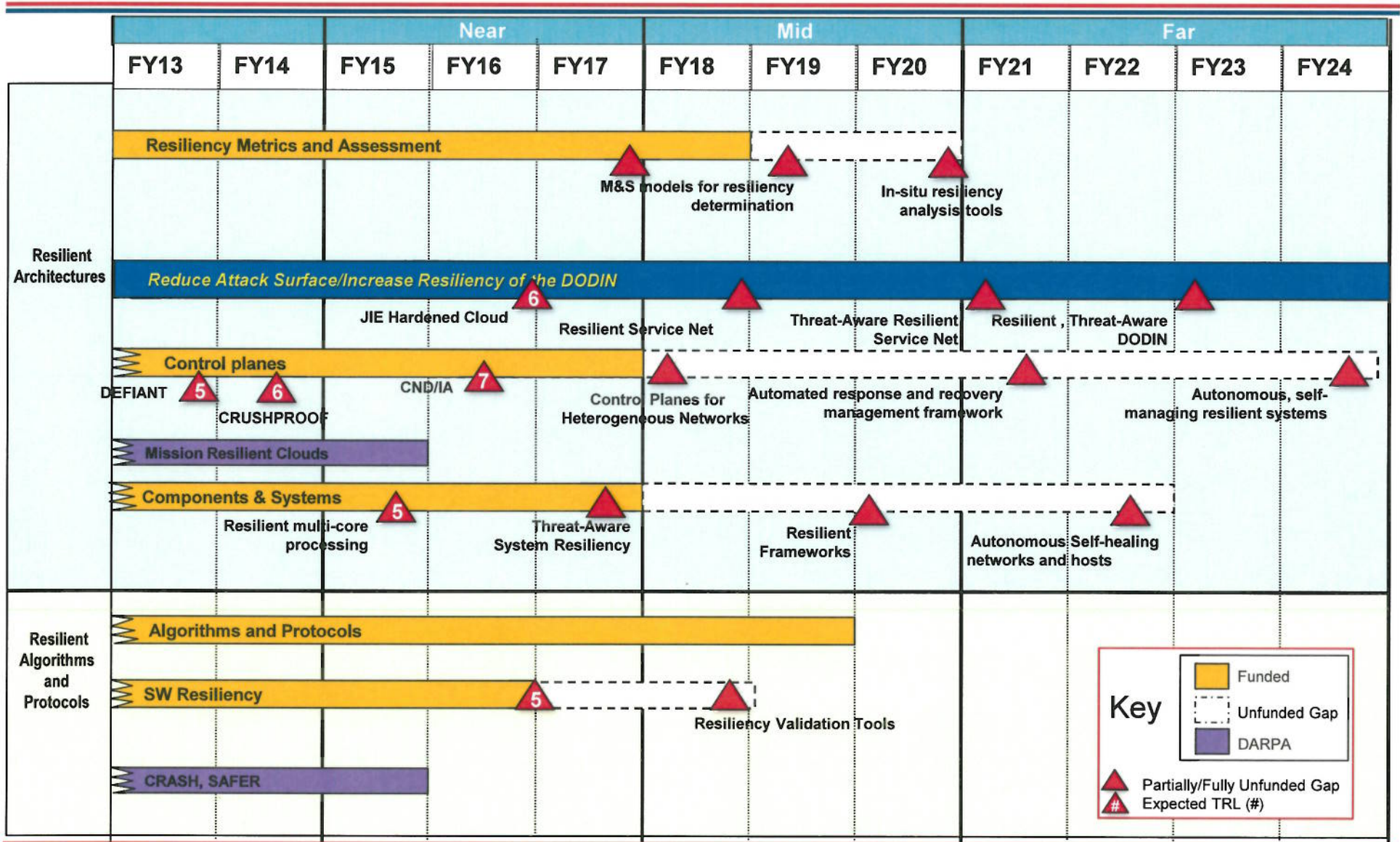

Accomplishments:

- 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

	Near					Mid			Far			
	FY13	FY14	FY15	FY16	FY17	FY18	FY19	FY20	FY21	FY22	FY23	FY24

Resilient Architectures

Resiliency Metrics and Assessment

M&S models for resiliency determination

In-situ resiliency analysis tools

Reduce Attack Surface/Increase Resiliency of the DODIN — 6

JIE Hardened Cloud

Resilient Service Net

Threat-Aware Resilient Service Net

Resilient , Threat-Aware DODIN

Control planes

DEFIANT — 5

CRUSHPROOF — 6

CND/IA — 7

Control Planes for Heterogeneous Networks

Automated response and recovery management framework

Autonomous, self-managing resilient systems

Mission Resilient Clouds

Components & Systems — 5

Resilient multi-core processing

Threat-Aware System Resiliency

Resilient Frameworks

Autonomous Self-healing networks and hosts

Resilient Algorithms and Protocols

Algorithms and Protocols

SW Resiliency — 5

Resiliency Validation Tools

CRASH, SAFER

Key

|	
Funded	(orange)
Unfunded Gap	(dashed box)
DARPA	(purple)
Partially/Fully Unfunded Gap	(red triangle)
# Expected TRL (#)	

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
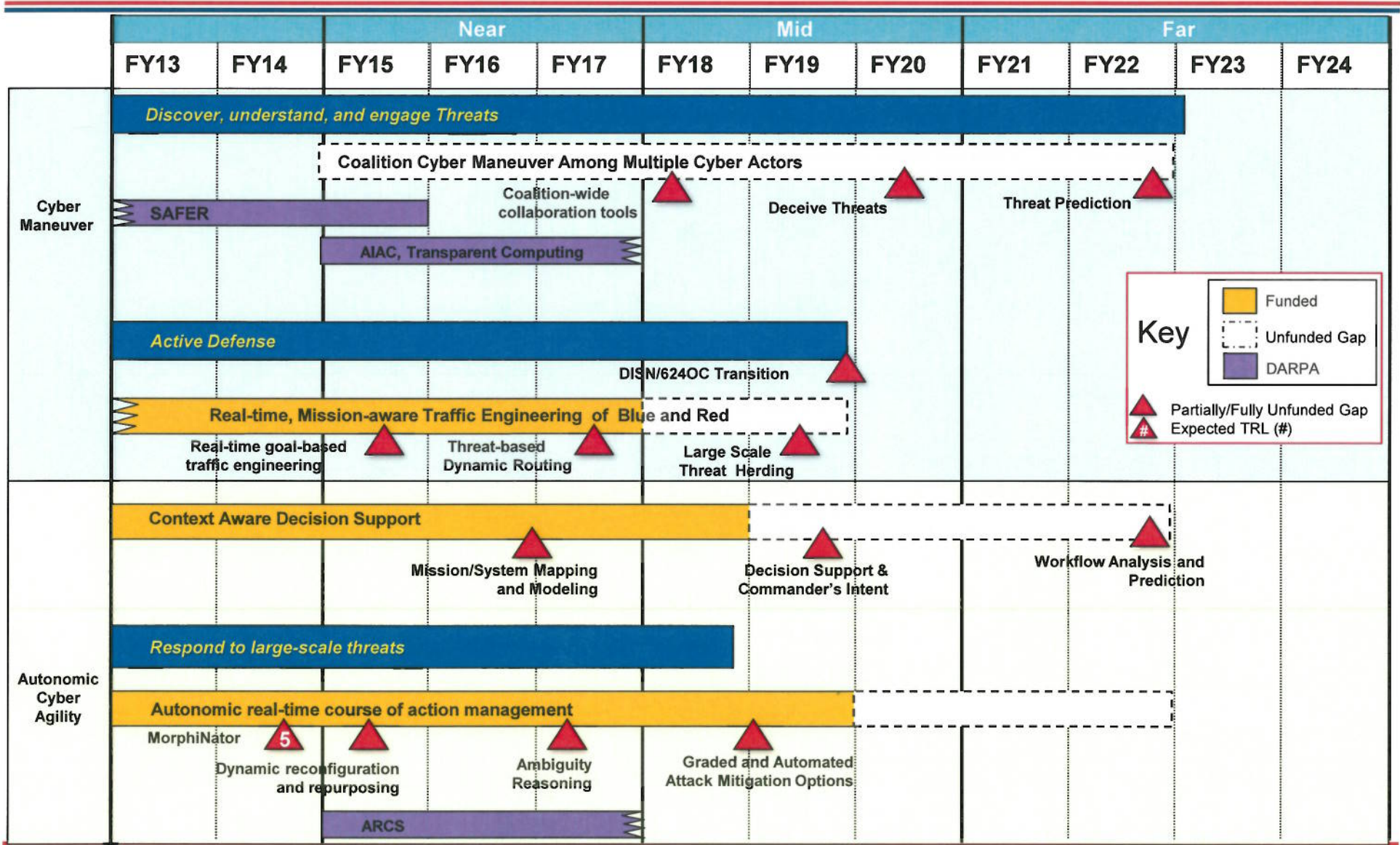- AF: ARCSYNE/COSYNE
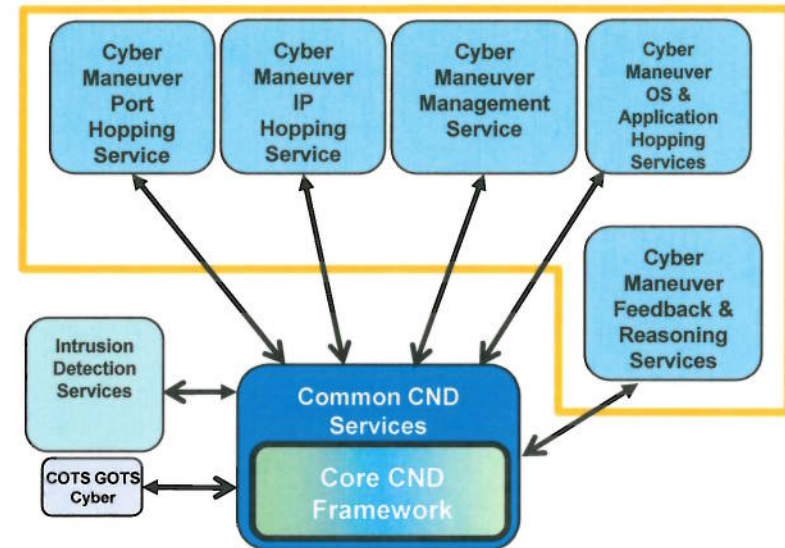
Technical Challenges:

- 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

	Near					Mid			Far			
	FY13	FY14	FY15	FY16	FY17	FY18	FY19	FY20	FY21	FY22	FY23	FY24

Cyber Maneuver

Discover, understand, and engage Threats

Coalition Cyber Maneuver Among Multiple Cyber Actors

SAFER

Coalition-wide collaboration tools

Deceive Threats

Threat Prediction

AIAC, Transparent Computing

Active Defense

DISN/624OC Transition

Real-time, Mission-aware Traffic Engineering of Blue and Red

Real-time goal-based traffic engineering

Threat-based Dynamic Routing

Large Scale Threat Herding

Autonomic Cyber Agility

Context Aware Decision Support

Mission/System Mapping and Modeling

Decision Support & Commander's Intent

Workflow Analysis and Prediction

Respond to large-scale threats

Autonomic real-time course of action management

MorphiNator — 5

Dynamic reconfiguration and repurposing

Ambiguity Reasoning

Graded and Automated Attack Mitigation Options

ARCS

Key

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

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
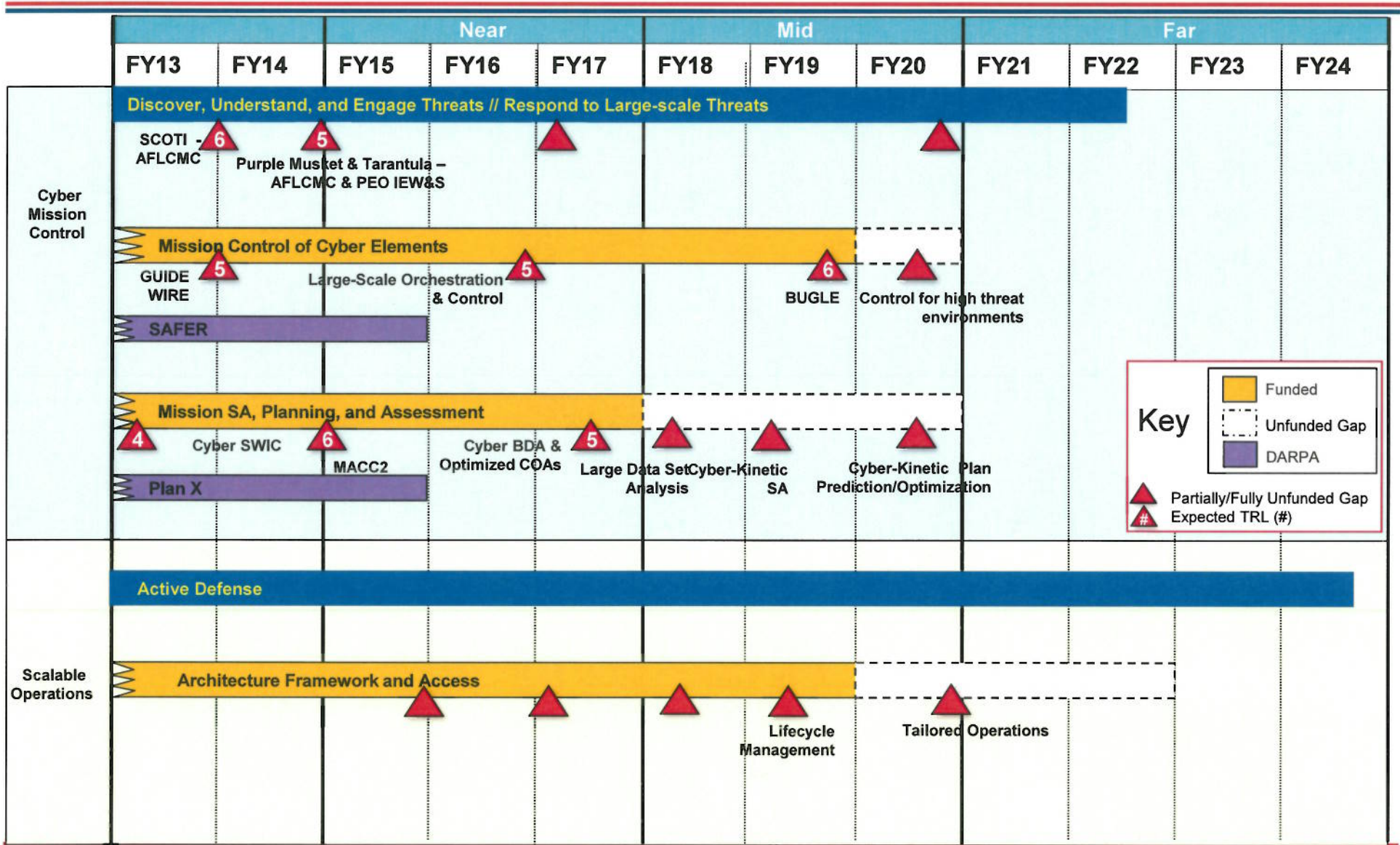

Accomplishments:

- 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, …)

Assuring Effective Missions Roadmap

	Near					Mid			Far			
	FY13	FY14	FY15	FY16	FY17	FY18	FY19	FY20	FY21	FY22	FY23	FY24

Cyber Mission Control

Discover, Understand, and Engage Threats // Respond to Large-scale Threats

SCOTI - AFLCMC **6** **5**

Purple Musket & Tarantula – AFLCMC & PEO IEW&S

Mission Control of Cyber Elements

GUIDE WIRE **5**

Large-Scale Orchestration **5** & Control

BUGLE **6** Control for high threat environments

SAFER

Mission SA, Planning, and Assessment

4

Cyber SWIC **6**

MACC2

Plan X

Cyber BDA & **5** Optimized COAs

Large Data Set Analysis

Cyber-Kinetic SA

Cyber-Kinetic Plan Prediction/Optimization

Scalable Operations

Active Defense

Architecture Framework and Access

Lifecycle Management

Tailored Operations

Key

Funded (orange)	Funded
Unfunded Gap (dashed)	Unfunded Gap
DARPA (purple)	DARPA
Red triangle	Partially/Fully Unfunded Gap
#	Expected TRL (#)

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

Analysis

Modeling & Simulation

Cyber Range

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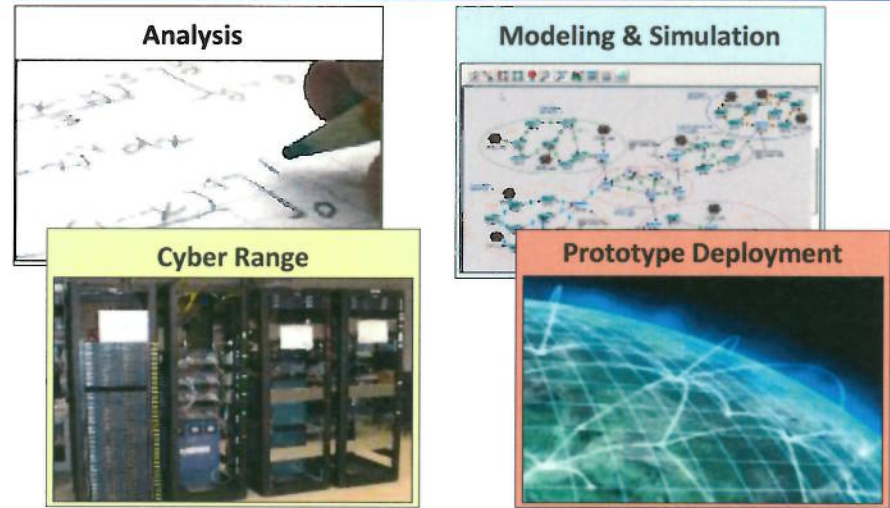
Accomplishments:
- Sequoia HPC achieved world record 10^{15} events/sec
- Army: Cyber Army Modeling & Simulation (CyAMS)
- AF: Cyber Experimentation Environment

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
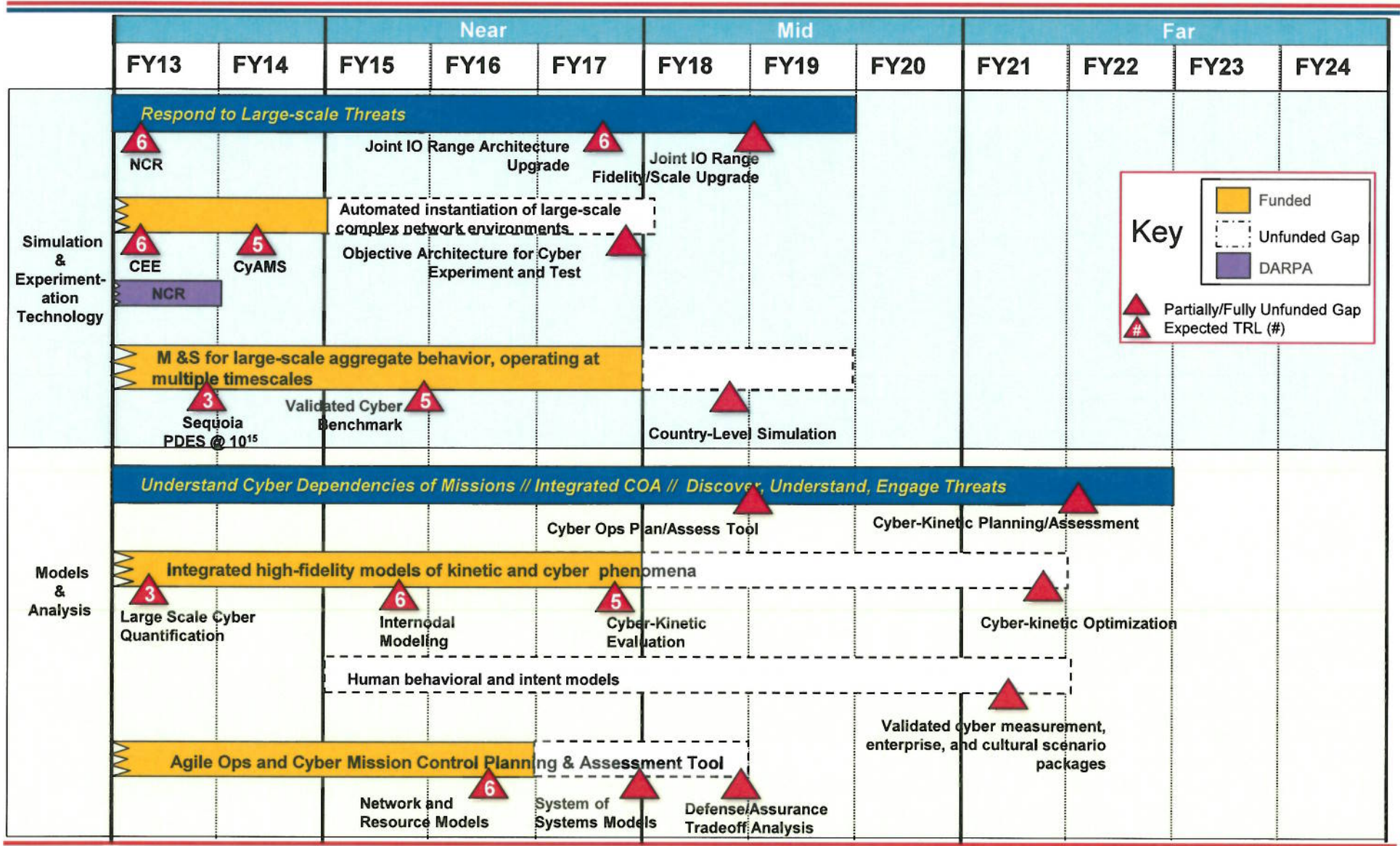
Distribution A – For Public Release

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**

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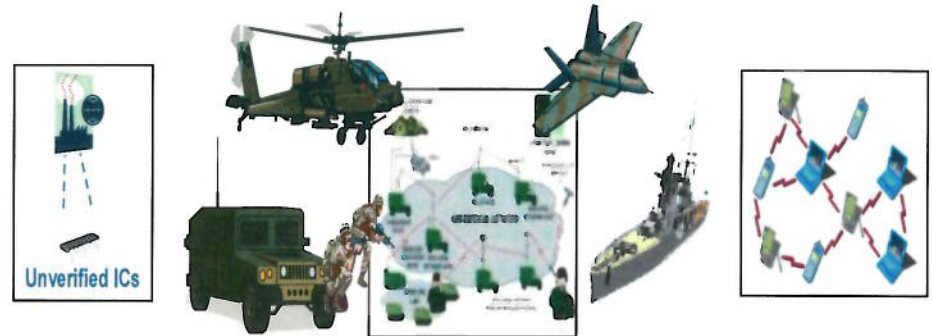
Apply the Cyber S&T Roadmap to Embedded, Mobile, and Tactical Environments

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

Embedded, Mobile and Tactical Roadmap

	Near					Mid			Far			
FY13	**FY14**	**FY15**	**FY16**	**FY17**	**FY18**	**FY19**	**FY20**	**FY21**	**FY22**	**FY23**	**FY24**

Mobile and Tactical Systems Security

Cyberspace Situational Awareness

Real-time tactical mission assessment tools

Assurance of Converged Mobile & Back-end Systems

Tactical security and assurance metrics — 4

Scalable, real-time analysis of trust in mobile devices and applications

Reduce Attack Surface/Increase Resiliency of Embedded/Tactical Systems

Certified DoD Apps/Store — 6

Certifiable Mobile OS

Agile code/OS reuse

Resilient Mobility

SMC — 6

Secure information sharing at tactical edge

APAC

TC

Protect Cyber-Physical Systems

Security for Real-Time Systems

Embedded Tactical Composite Trust

Reduce attack surface and increase resiliency of embedded/weapon systems

Network Pump II — 7   TACDIS — 7

Composed embedded system security measurement tools

Trusted embedded systems at tactical edge

Secure Embedded System Architectures

Architectural approaches — 4

Prototypes for secure mobile devices and infrastructure

HACMS, APAC

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

Defense	Engagement
Reduce attack surface and increase resiliency of DODIN	Active defense
Reduce attack surface and increase resiliency of embedded/weapons systems	Respond to large-scale threats
Discover, understand, and engage threats	

Situational Awareness and Courses of Action

| Cyberspace situational awareness | Understand cyber dependencies of missions | Integrated course of action, cyber and non-cyber |

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

Terms:
ICD: Initial Capabilities Document
RDA-TF: Research, Development, & Acquisition Task Force
TTCP: The Technical Cooperation Panel

Distribution A – For Public Release

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

- ## Telecommunications/Wireless
  - Telecommunications Labs (CERDEC)
  - Communications System Integration Laboratory (CSIL)
  - HI-FI Advance Waveform and Cyber laboratory
  - Electromagnetic Environment (EME)

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

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

DoD Cyber Transition to Practice (CTP) Initiative

Emerging "Best of Breed" S&T Matured through Cyber Range-based T&E, Demonstrations, and Operational Pilots
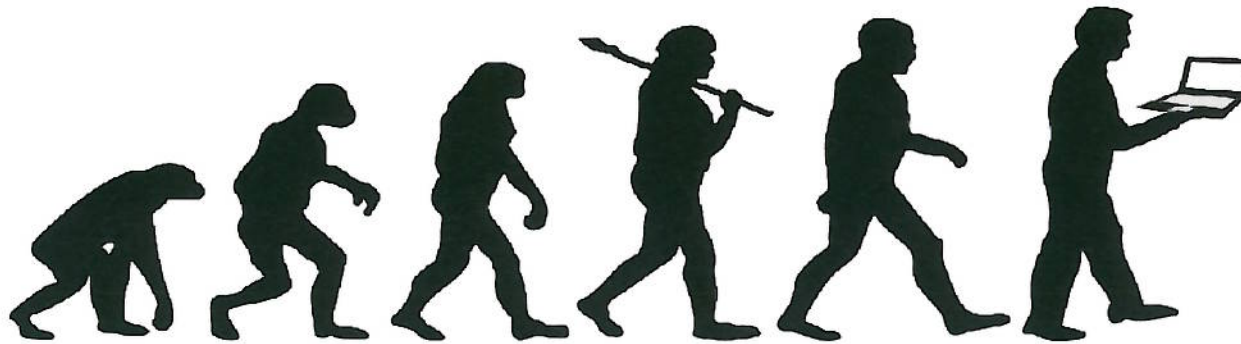
- **CTP is maturing and transitioning DoD-funded cyber S&T**
  - Get S&T addressing key gaps into Ops
  - White House priority
  - Increase TRL, reduce risk
- **CTP emphasizes:**
  - Rapid results near term
  - Committed transition partner(s)
  - Co-funding by transition partner(s)

- **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

Improve Industry understanding of DoD needs

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
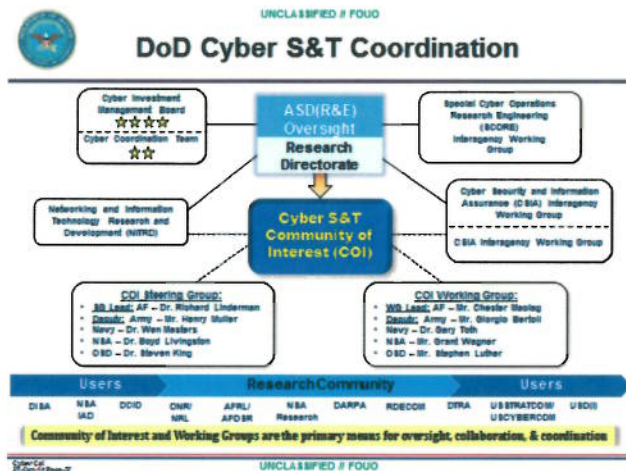- DoD IR&D SEARCH Trends

www.DefenseInnovationMarketplace.mil

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)

  - Air Force Office of Scientific Research (AFOSR) (http://www.afosr.af.mil)

  - Defense Advanced Research Projects Agency (DARPA) (http://www.darpa.mil)

Contacts

UNCLASSIFIED // FOUO
DoD Cyber S&T Coordination

- ## 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

- ## 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

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

ACADEMIA

DOD LABS

DARPA

DOD PROGRAMS

GOOD IDEAS

Large Defense Contractors

Small Businesses

System Integrators

Trusted Hardware/Software Manufacturing

Information Technology Vendors

Venture Capitalists

Non-traditional Defense Companies

PRODUCTS

Business Systems

Data Systems

High Performance Computing Systems

IT Systems

Weapon Systems

Many More...

DOD CUSTOMERS