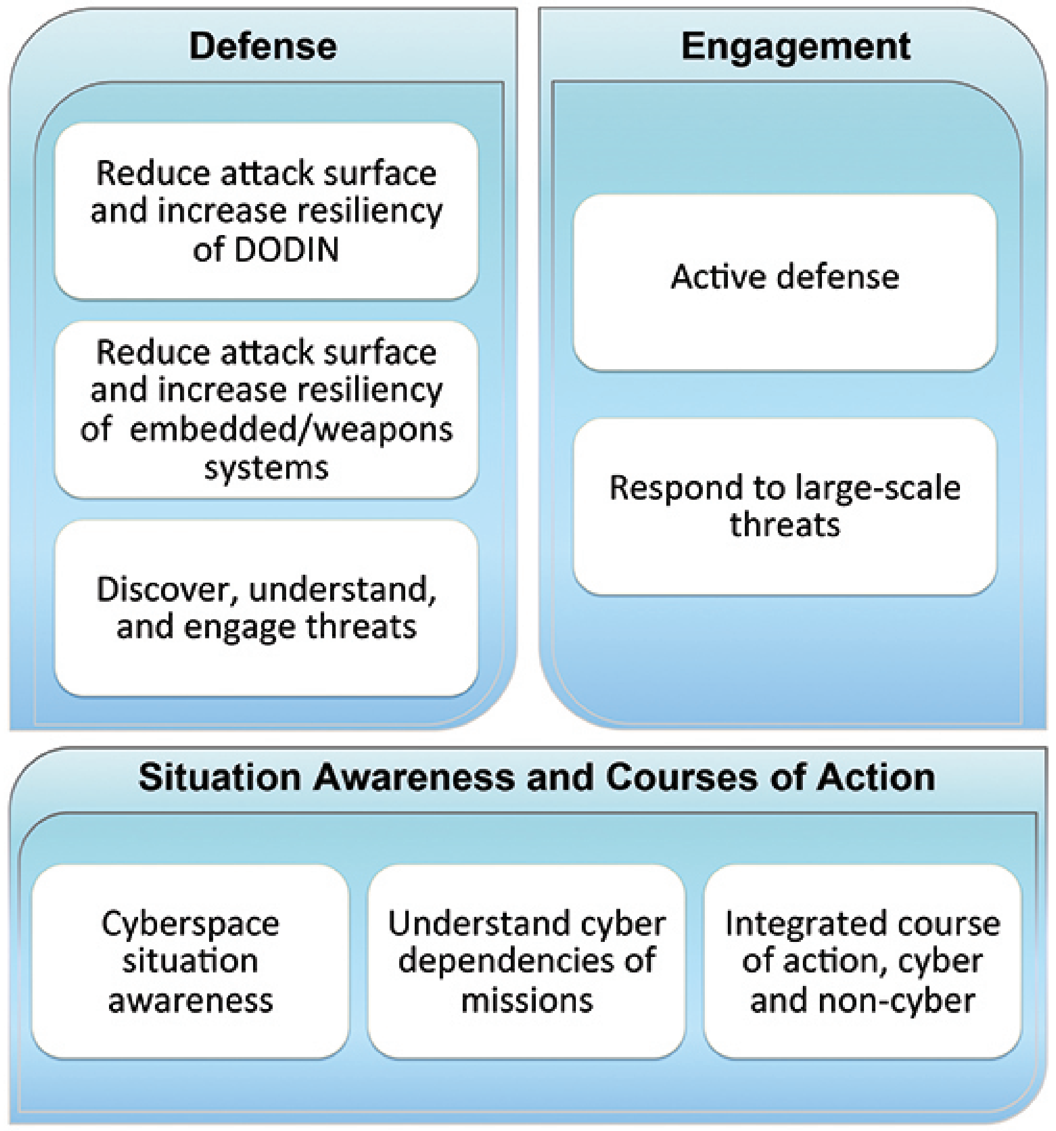
Cyber Community of Interest (COI)

- Provides a forum for coordinating cyber S&T strategies
- Jointly plans programs across the Department
- Leads the discovery, development, and integration of Cyber S&T
- Measures and reports Cyber S&T progress to the DoD leadership
- Addresses full spectrum DoD operations and National Security Objectives

Cyber S&T Capability Framework



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

Situation Awareness and Courses of Action

Cyberspace situation awareness

Understand cyber dependencies of missions

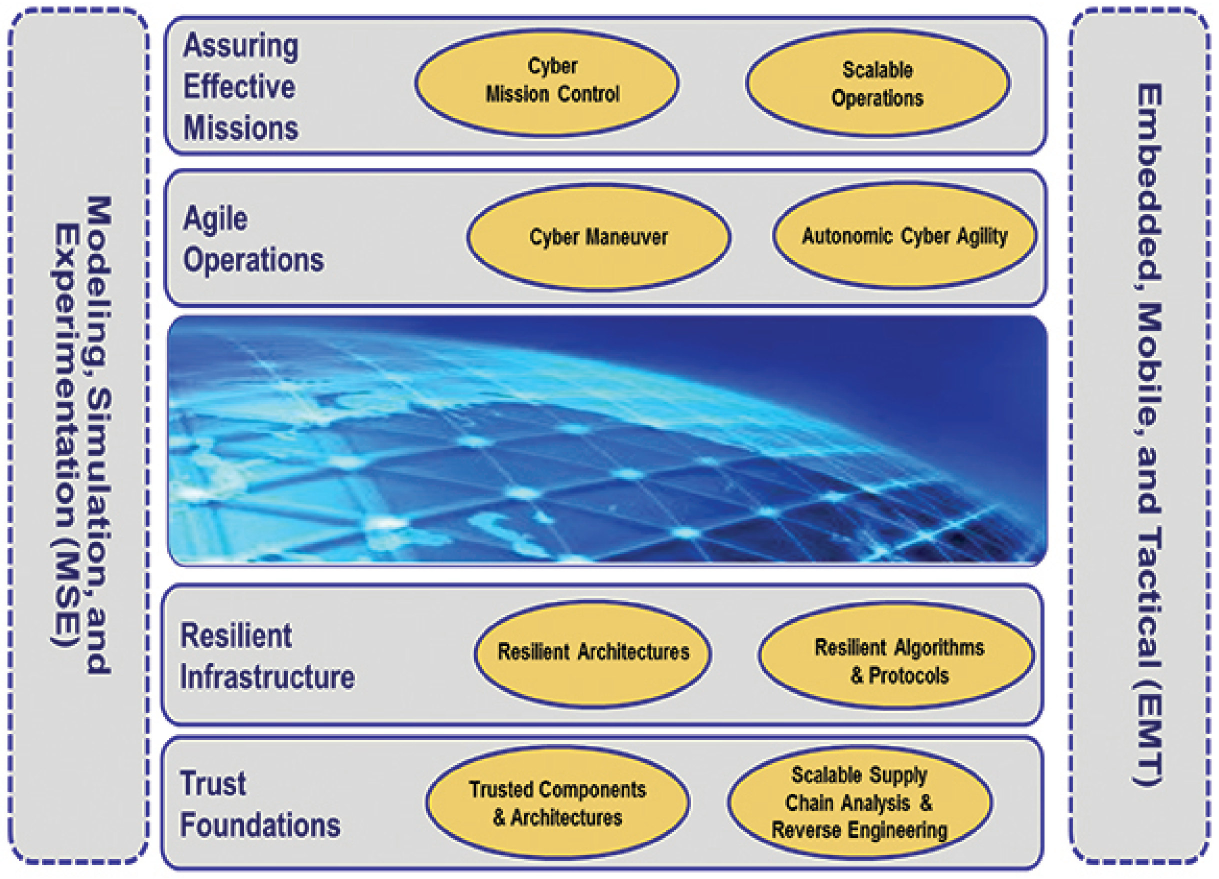
Integrated course of action, cyber and non-cyber

The S&T Capability Framework is derived from the Joint Staff Operational Activity Framework. The Cyber COI S&T Roadmap enables Defense, Engagement, and Situation Awareness & Course of Action planning. The Roadmap also includes developmental enablers for S&T, such as modeling, simulation, experimentation, and metrics.

COI Steering Group Members:

AF: Dr. Richard Linderman (Lead)
OSD: Dr. Steven E. King
ARMY: Mr. Henry Muller
NAVY: Dr. Wen Masters
NSA: Dr. Boyd Livingston

Thrust 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 & Protocols

Trust Foundations: Trusted Components & Architectures; Scalable Supply Chain Analysis & Reverse Engineering

Embedded, Mobile, and Tactical (EMT)

Main Thrusts:

Assuring Effective Missions (AEM): Assess and 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, and sustain or recover critical functions

Trust: Establish known degree of assurance that devices, networks, and cyber-dependent functions perform as expected, despite attack or error

Cross Cutting Areas:

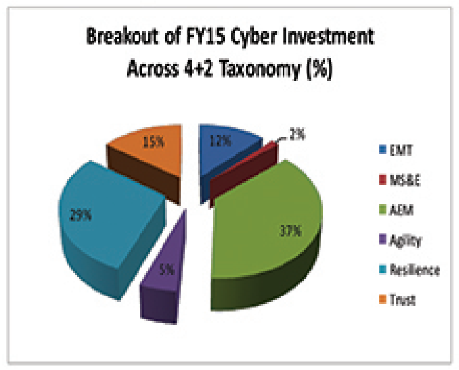
Embedded, Mobile, & Tactical (EMT): Increase the capability of cyber systems that rely on technologies beyond wired networking and standard computing platforms

Modeling, Simulation, & Experiment (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

Gaps & Opportunities

Areas for Targeted Growth

- Modeling, Simulation, Experimentation, & Metrics
- Manageable Agility
- Integrated Cyber-EM Operations
- Trusted embedded systems of mixed pedigree



Specific Gap Assessment

Defense:

- Trustworthy embedded system architectures composed of components of mixed trust pedigree
- 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

Situation 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

Engagement Opportunities

- Cyber-Security Information Analysis Center (CS-IAC)
- IR&D Engagements via Defense Innovation Marketplace
- Cooperative Agreements
- SBIR Program
- Specialized Ranges
- Cyber Transition to Practice
- TTCP Cyber Security Grand Challenge

This briefing is Approved for Public Distribution. 88ABW-2015 1092 2015 03 16