



# Cyber Community of Interest

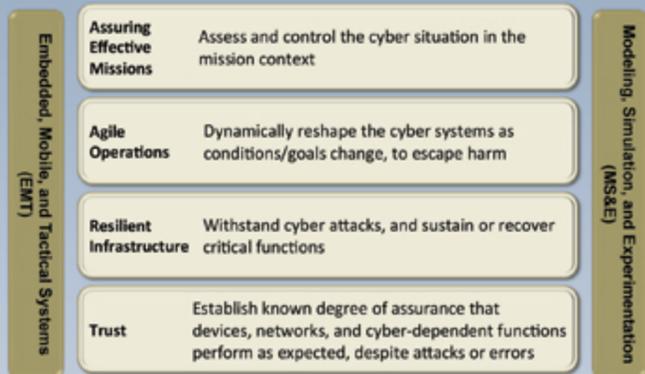


## Scope/Thrust Areas

Desired Capabilities from Cyber S&T:  
Capability Based Cyber S&T Framework



## Cyber S&T Areas and Impact on Capabilities



EMT and MS&E are cross cutting areas that the COI identified as in need of special attention

## Success Stories

Trust	Resilience and Agility
<ul style="list-style-type: none"> <li>SW Assessment: Enterprise, Tactical, Mobile</li> <li>Host Integrity at Startup and Runtime using Kernel Monitoring</li> <li>Tactical PKI</li> <li>Cross Domain Solutions: Enterprise Clients and Servers, Tactical, Very Small SWAP for Tactical Edge</li> <li>OS and CPU Independent Defense of Embedded Systems and Control Systems</li> </ul>	<ul style="list-style-type: none"> <li>Fault Tolerant Computing and Byzantine Fault Tolerance</li> <li>Software Based Flexible Encryption</li> <li>Distributed, Assured, and Dynamic Configuration</li> <li>Dynamic Reshaping of Software Execution across Heterogeneous Systems Architecture</li> <li>Machine Learning Techniques for Traffic Anomaly Detection and Automated Actions</li> </ul>

Assuring Effective Missions		
Situation Awareness	Mission Mapping	COA and Cyber Operations
<ul style="list-style-type: none"> <li>Data Ingestion and Analytics, Enterprise and Tactical</li> <li>Visualization</li> <li>Malware Analysis Tool for Detection, Analysis and Classification of Signatures</li> <li>Control Systems Monitoring</li> </ul>	<ul style="list-style-type: none"> <li>Mission Mapping and Cyber Key Terrain Analysis</li> </ul>	<ul style="list-style-type: none"> <li>Mission Cyber Framework</li> <li>Integrated Resilient Architecture for Cyber Operations</li> <li>Large Scale Orchestration and Control</li> <li>Global Coordination</li> </ul>

## Impact

Significant Reductions in Capability Gaps

- Secure Data Transfer Across Classification Boundaries via Innovative Cross Domain Solutions for Enterprise, Tactical as well as Tactical Edge
- Hardened Attack Surface via Innovative Software Assessment before Deployment, at Startup, and at Runtime
- Dynamic Reshaping of SW Execution and System Configurations to Provide Resilience Against Cyber Attacks
- Fault Tolerant Computing to Increase Resilience

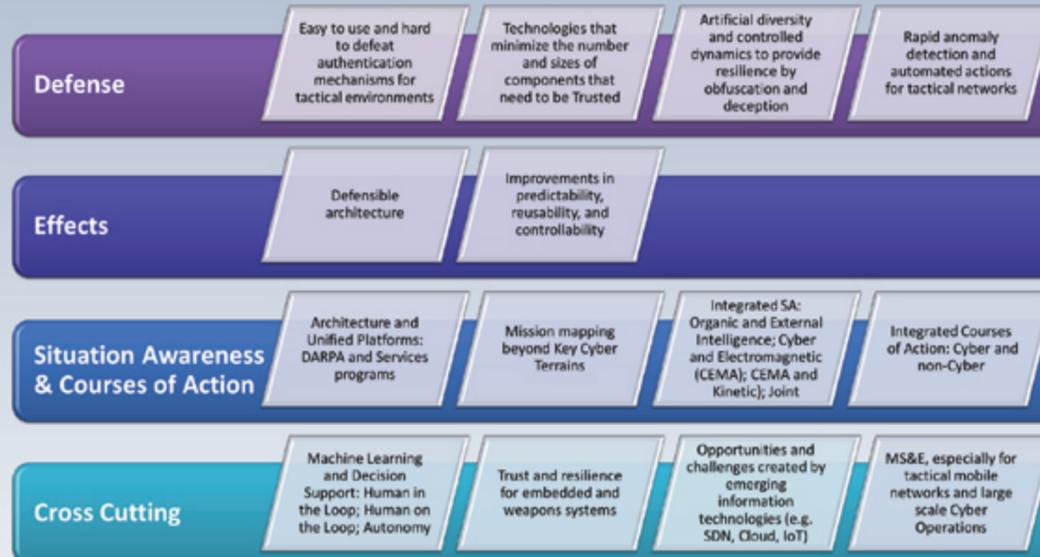
Increased Mutual Reliance and Investment Leverage

- Strategies and Roadmaps Coordinated Across Services, NSA & OSD
- Complementary Research Priorities Developed to Build Mutual Reliance and Multiply the Estimated Technology Output
- Several Inter-Services Agreements Signed to Integrate Technologies from Two or More Services to Develop New and/or Improved Capabilities
- ASD R&E Funded New Starts (Seedlings) Responsible for Many New Programs and Technologies
- Helped OSD with Cyber Transition to Practice Initiatives and Nominated Several Programs

Shifted Technical Focus

- Proactively Added MS&E and EMT as Important Cross Cutting Thrust Areas in the Roadmaps

## Focus Going Forward



## Cyber COI Membership

### Steering Group Members:

Army: Mr. Henry Muller (Lead)  
Navy: Dr. Wen Masters (Deputy)  
Air Force: Mr. Chester MacIag  
OSD: Dr. Steven King  
NSA: Ms. Cheryl Mawhinney  
DARPA: Mr. E. Dick Urban

### Working Group Members:

Army: Dr. Bharat Doshi (Lead)  
Navy: Dr. Gary Toth (Deputy)  
Air Force: Ms. Anna Weeks  
OSD: Dr. Paul Lopata  
NSA: Mr. Philip D'Ambrosio

## Engagement Opportunities for Industry

### Performers for DoD Cyber S&T

Services S&T Labs: AFRL, RDECOM/CECOM, NRL, SPAWAR

DoD Agencies: NSA/R

DOE Labs, Academia, FFRDCs and UARCs

Industry Players

- Defense Industrial Base
- Non-traditional (non-DoD uses are key drivers of Cyber technologies)
- Small companies with key Cyber expertise and products

- About 70% of DoD S&T funds are expended by industry and academia and 10% by FFRDCs/UARCs
- Increasing emphasis on leveraging industry expertise and technologies



### Example Technologies of Interest

- Technologies for Integrated Cyber Situation Awareness (Organic data and external intelligence)
- Analytics on multi-source, multi-time scale data in structured and unstructured formats
- Machine learning applied to anomaly detection, situation awareness, and course of action
- Technologies for easy to use multifactor authentication in tactical networks
- Technologies for increasing autonomic Cyber resilience via obfuscation, deception, and evasion
- Minimizing the set of computing and communications components that need to be trusted
- Lightweight monitoring and analysis within mobile devices
- Technologies for Detection of smart malwares (e.g. with Polymorphic and Metamorphic capabilities)
- Cyber security of IoT, Cyber Physical systems, and emerging information technologies



### Engagement Mechanisms & Sources of Information

- Direct engagement with Services S&T: IR&D feedback; closer look at needs; BAAs. COI POC can help
- FedBizOpps: Industry Days, RFIs, RFPs, BAAs, and other opportunities <http://www.FedBizOpps.Gov>
- Defense Innovation Marketplace <http://www.defenseinnovationmarketplace.mil/index.htm>
- Cyber Security and Information Systems Information Analysis Center <https://www.csiac.org/>
- Cooperative Agreements, SBIR/STTR
- Specialized ranges offered to industry for T&E and risk reduction
- DIUx, Army Silicon Valley Outreach, ARL West, Army Innovation Challenge, AFRL commercialization academy, etc.

