NDIA S&ET Conference

Cyber COI Strategic Overview

18-20 APR 2017

Mr. Gary Blohm (SG Lead)

Dr. Bharat Doshi (WG Lead)

Leadership and Membership

Steering Group Members

- *Army:* Mr. Gary Blohm (Lead)
- *Navy:* Dr. Wen Masters (Deputy)
- *Air Force:* Mr. Daniel Goddard
- *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

Cyberspace

- **Cyberspace: Domain characterized by the use of electronics, electromagnetic spectrum, and software to store, modify, and exchange data via networked systems and associated physical infrastructure.**
- **Cyberspace is relatively new, fast growing, and dynamic**
  - Rapid growth of user base
  - Rapid insertion of new technologies
  - Rapid growth of new applications
- **Pervasive underpinning of nearly all personal life, business, public services, national security, and defense functions, across all phases of shaping and conflict.**
- **Reliance on the Cyberspace is growing rapidly.**

Cyberspace Growth, Ubiquity, & Dynamics:
Personal, Commercial & Public Services

- **Global Internet**
- **Wi-Fi, Cellular telephony and data**
- **Critical Infrastructures (e.g. Energy, Transportation, Finance, and Communication)**
- **IoT, wearable electronics, machine-machine and man-machine systems, Autonomous Systems**
- **Brain-machine, Brain-brain**

Cyberspace Growth, Ubiquity, & Dynamics: DoD/IC

- Interactive DODIN and other mission networks
  - Ground, air, space, underwater/surface
  - Wired, wireless, mobile
  - PNT, C2, Logistics, Fire, Medical, Situation Awareness
- Energy and power systems
- Ground, Sea, Air, and Space platforms
- Weapons systems
- Distributed sensor networks
- Machine-machine communication and unattended embedded systems
- Man-machine and Autonomous Systems (Robots, UAVs, UUVs, Swarms)
- Brain-machine and brain-brain communication

Cyberspace, Cyber S&T, Cyber COI and Relationships with Other COIs

- **Other COIs deal with technologies that create new cyberspace capabilities and applications**
- **However, cyberspace is vulnerable to cyber attacks that lead to adverse impact on the mission via**
  - Loss of service (Availability)
  - Exfiltration of vital information (Confidentiality and Privacy)
  - Corruption of information (Integrity)
  - Loss of control; Destruction or malfunction
- **New vulnerabilities surface as new cyberspace technologies and applications are introduced.**
- **Cyber COI S&T is aimed at novel approaches and technologies to secure current and new cyberspace applications, and to create desired effects on the adversary cyberspace.**

Goals of Cyber S&T

- **Technologies that autonomously prevent the adversaries from accessing blue cyberspace and minimize the adverse impact if the adversary succeeds.**
- **Technologies that maximize the effects on the adversary missions via cyberspace operations.**
- **Technologies and tools to help Cyber Mission Force teams conduct winning DCO and OCO**
- **Technologies and guidelines for proactively developing architectural and design principles, sensors, and analytics to ensure that emerging and future cyberspace are secure.**

Cyber COI Taxonomy and Tier 1 S&T Areas

Protection

Trust: Prevention of undesirable access to blue cyberspace. **Autonomic Cyber Resilience:** Minimizing mission impact. **Local Sensors, Analytics, and Actions**

Effects

Successful effects in presence of adversary defenses

Cyber Situation Awareness

Technologies for collection and fusion of data from multiple sources. Analytics, machine learning, and deep learning for intrusion detection, attribution, and BDA. Echelon and role specific visualization.

(Decision Support for) Cyber C2

Mission mapping. Tools for COA. Technologies, platforms, and tools for collaborative planning and evaluation of strategic and tactical plans in cyberspace.

Key Investment Trends

Demand signals from Cyber Mission Force Teams and other operational communities. ➔ **Increasing S&T for Cyber SA and Cyber C2**

Increasing role of cyberspace in platforms and weapons systems ➔ New vulnerabilities, consequences, and OODA loop ➔ **increasing S&T for cyber operations on DoD Cyber Physical systems**

Projected exponential growth in low cost, small SWaP, connected devices in commercial and DoD applications (Internet of Things) ➔ **Increasing S&T for cyber operations on DoD IoT**

Rapidly decreasing cost of providing controlled dynamics in low level functions ➔ **Increasing S&T for the use of the dynamics to provide obfuscation, deception, and evasion for increasing adversary work factor**

Shrinking OODA loop, cognitive overload, and multi-source data/intelligence ➔ **Increasing S&T for machine learning and autonomy in cyber defense/offense**

- **Predictability, reusability, and controllability of effects**
- **Modeling human dimensions**

Success Stories

Protection

- SW assurance: Pre-Deployment, Boot Time, Run Time
- PKI for Tactical, Including Non-Person Entities
- Cross-Domain Solutions (CDS) for Enterprise, Tactical, and Tactical Edge
- Extremely Lightweight Intrusion Detection Systems (IDS): Tactical and Tactical Edge
- System-on-the-Chip Reprogrammable Encryptor
- Cyber Defense of Microprocessors and Controllers
- Byzantine Fault Tolerance for Control Systems Resilience
- Formal Methods for Cyber Physical Systems

Effects

- Integrated Cyber Electro-Magnetic Effects
- Resilient OCO

Cyber Situation Awareness

- SCADA Sensors and Remote Monitoring
- Code Attribution via Analysis of Coding Style
- CEMA SA Framework and Analytics
- Universal Composable Visualizer for SA

(Decision Support for) Cyber C2

- Cyber C2 Through Graph Visualization
- Integrated CEMA Operations Specifications
- Scalable Cyber Technology Integration
- Cyber Operations Architecture

Impact

Significant Reductions in Capability Gaps

- Secure Cross Domain Data Transfer
- Hardened Attack Surface via Static and Dynamic SW Assurance
- Cyber Resilience via Reconfiguration, Obfuscation, Deception, and Fault Tolerance
- Situation Awareness Framework and Analytics
- Low Level SA, Actions, and Recovery

Increased Mutual Reliance and Investment Leverage

- Coordinated Cyber S&T Strategies and Roadmaps
- Complementary Cyber S&T Priorities for SA & C2
- Complementary Cyber S&T Priorities for Platforms and Weapons Systems

Shifted Investment Focus

- Increased S&T for Cyber SA and C2, and Cyber Defense/Offense for Platforms and Weapons Systems
- Stronger Interest in Machine Learning and Autonomy for Cyber Defense and Offense
- Growing Interest in Human Dimensions in Cyber Operations

S&T Focus Going Forward

Protection

- Novel Authentication Mechanisms for Tactical Environments
- Automated Obfuscation, Deception, and Maneuvers
- Automated Intrusion Detection and Actions for Tactical Networks

Effects

- Predictability, Reusability, and Controllability
- Resilience and Morphability

Cyber SA

- Integrated SA: Multi-Service; Organic and External Intelligence; Cyber and Electromagnetic; Cyber, EW, and Kinetic

(Decision Support for) Cyber C2

- Architecture and Unified Platforms
- Integrated Course of Action: Cyber and Non-Cyber

Enablers

- Machine Learning and Autonomy
- Human Dimensions

Cyber Defense/Offense for IoT, Platforms, and Weapons Systems

Performers for DoD Cyber S&T

- **Services and Agencies S&T Labs: AFRL, NRL, NSA, RDECOM**
- **DOE Labs, FFRDCs, and UARCs**
- **Academia**
- **Industry Players**
  - Defense Industrial Base
  - Non-traditional
  - Small Companies with Key Expertise and Products
- **About 70%-80% Extramural**
- **Emphasis on Leveraging Industry and Academic Expertise**

Engagement Opportunities for Industry: Engagement Mechanisms & Sources of Information

- **Direct Engagement with Services S&T via feedback on IR&D plans and technology directions.**
- **www.FedBizOpps.Gov: Industry Days, RFIs, RFPs, BAAs.**
- **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**
- **T&E and Risk Reduction**