RELIANCE 21 – DoD COMMUNITIES OF INTEREST

CYBER

Scope/Thrust Areas

**Protection**
- Prevention of adversarial access to the blue cyberspace. Autonomic Cyber Resilience to Contain Mission impact. Local Sensors, Analytics, and Actions.
- Successful effects in presence of adversary defenses.

**Cyber Situational Awareness (Cyber SA)**
- Collection and fusion of data from multiple sources; Analytics for intrusion detection, attribution, and Battle Damage Assessment (BDA). Echelon role specific visualization.

**Cyber Command and Control (Cyber C2)**

Impact on Capability Needs

- Secure Cross Domain Data Transfer
- Hardened Attack Surface via Static and Dynamic Software (SW) Assurance
- Low Level SA, Actions, and Recovery
- Situation Awareness Framework and Analytics
- Lead, Invest Service(s)/agency identified for Cyber SA, Cyber C2, Platforms and Weapons Systems, and Low Cost Low Resource Devices. Other Services/agency will Leverage
- USD(R&E) funded starts responsible for many new collaborative programs
- Increased S&T for Cyber SA and C2, and Cyber for Platforms and Weapons Systems
- Stronger Interest in Machine Learning and Autonomy for Cyber Defense and Offense

Engagement Opportunities for Industry

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

Example Technologies of Interest
- Easy to Use Multifactor Authentication in Tactical Networks
- Analytics on Multi-source, Multi-time Scale Data
- Machine Learning and Autonomy for Anomaly Detection, Situation Awareness, and Cyber Maneuvers
- Autonomic Cyber Resilience via Obfuscation, Deception, and Evasion
- Lightweight Monitoring and Analysis in Mobile Devices.
- Detection of Smart Malwares
- Cyber Security of IoT and Cyber Physical Systems
- Cyber Working Group Lead: Dr. Bharat Doshi, bharat.t.doshi.civ@mail.mil

Focus Going Forward

**Protection**
- Novel Authentication Mechanisms for Tactical Environments
- Automated Discovery and Repair of Vulnerabilities
- Obfuscation, Deception, and Maneuvers
- Automated Intrusion Detection and Actions

**Effects**
- Predictability, Reusability, and Controllability
- Resilience and Morphability

**Cyber SA**
- Integrated SA: Multi-Sector; Organic and External Intelligence; Cyber and Electromagnetic; Cyber, EW, and Kinetic
- Cyber Battle Damage Assessment (BDA) Cyber C2
- Architecture and Platforms
- Integrated Course of Action: Cyber and Non-Cyber

**Cross Cutting**
- Machine Learning
- Autonomy
- Human Dimensions

Success Stories

**Protection**
- Software and Firmware De-Bloating
- Defense of Embedded Firmware via Symbiotes
- Hybrid Binary/Ternary Computing
- Public Key Infrastructure (PKI) for Tactical, including Non-Person Entities
- Extremely Lightweight IDS; Tactical and tactical edge
- System-on-the-Chip Reprogrammable Encryptor
- Cyber Defense of Microprocessors and Controllers
- Autonomic Recovery of Programmable Logic Controllers

**Effects**
- New Effects Technologies in Operational Use
- Resilient Offensive Cyber Operations (OCO)

**Cyber SA**
- SCADA Sensors and Remote Monitoring
- Code Attribution via Analysis of Coding Style
- Post Compromise SA-Tools
- Universal Composable Visualizer

**Cyber C2**
- Cyber C2 Through Graph Visualization
- Integrated Cyber Electromagnetic Activities (CEMA) Operations Specifications
- Cyber Physical Systems: Information and Intelligence
- Cyber Mission Assurance