U.S. ARMY COMBAT CAPABILITIES DEVELOPMENT COMMAND – ARMY RESEARCH LABORATORY

Cyber Security Collaborative Research Alliance (CRA) Overview

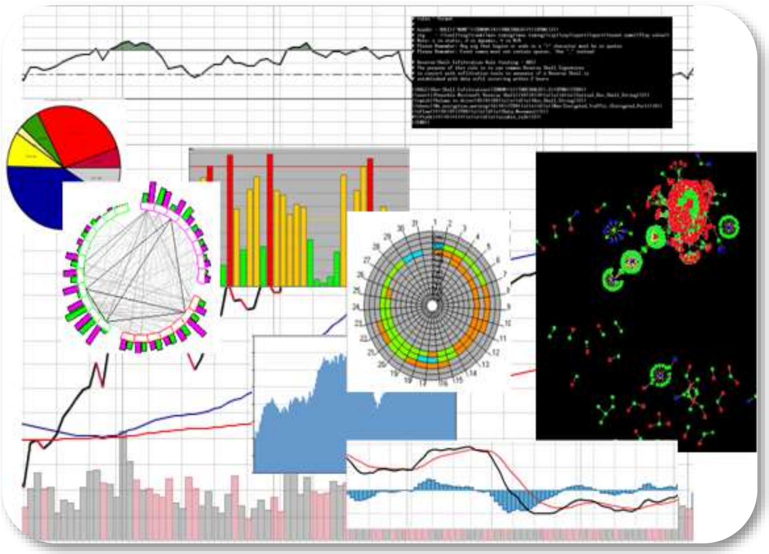
CYBER SECURITY CRA

A collaborative Alliance between CCDC ARL, C5ISR Center, Academia, and Industry to advance the foundation of cyber science in the context of Army networks

Cyber Security CRA Objectives

- **Develop a fundamental understanding of cyber phenomena (incl. human aspects)**
- **Fundamental laws, theories, & theoretically grounded & empirically validated models**
- **Applicable to a broad array of Army domains, applications, and environments**

- Collaborative Research Alliance (CRA) awarded Sept. 2013
- Applied Research & Experimentation Partner (AREP) awarded Oct. 2014



SCOPE & CHALLENGES

Domain:

- Heterogeneous & convergent networks
- Army must:
  - Adapt to rapidly changing technologies, tactics, & threats
  - Maintains situational awareness across complex networks
  - Be able to use and defend networks that it neither owns nor directly controls
  - Construct mission networks with a variety of partners & allies

Army Challenges:

- Large attack surface
- Relatively disadvantaged assets
- Large scale & high dynamics
- Advanced persistent threats
- Close proximity with threats
- Disadvantaged users
- Complex, adversarial, and uncertain environments

Warfighter Payoff:

- Resilient, secure, intelligent networks in dynamic and hostile battlefield environments
- Advanced methods and tools for intrusion detection that are rapidly deployable and customizable
- Techniques and strategies to continually increase complexity and cost to attackers attempting to compromise friendly networks

PROGRAM STRUCTURE

DEVCOM ARMY RESEARCH LABORATORY

Cyber Security Alliance

DEVCOM ARMY RESEARCH LABORATORY

DEVCOM C5ISR CENTER

CYBER-SECURITY COLLABORATIVE RESEARCH ALLIANCE

Consortium

PennState

Consortium Lead

Carnegie Mellon University

UC DAVIS UNIVERSITY OF CALIFORNIA

UNIVERSITY OF CALIFORNIA UC RIVERSIDE

perspecta

INDIANA

NORTHEASTERN UNIVERSITY BOSTON, MASSACHUSETTS

IBM

UTEP

HBCU/MI Partnered Research Initiative award to U. Texas, El Paso, Sept. ‘16

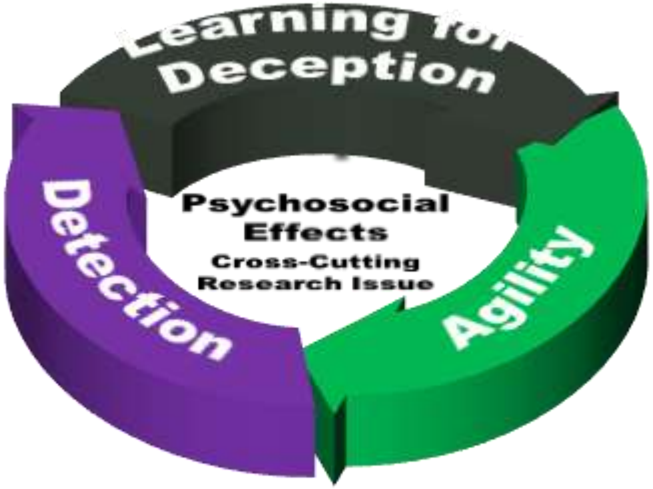
Applied Research & Experimentation Partner

- Lead: Perspecta Labs
- Supports CCDC C5ISR/ARL Cyber Enterprise
- Supports CRA with applied research & experimentation
- Accelerates transition

RESEARCH FOCUS

Develop an understanding of cyber phenomena:

- **Fundamental laws, theories, & theoretically grounded & empirically validated models**
- **That can be applied to a broad range of Army domains, applications, & environments**



Research Areas:

- **Detection:** Theories & models that relate properties & capabilities of cyber threat detection & recognition to properties of malicious activity.
- **Agility:** Theories & models to support planning and control of cyber maneuvers in the space of networks, network characteristics, platforms, topologies and software.
- **Learning for Deception:** Theories & models that relate fundamental properties and capabilities of adaptive deception techniques for defense and mission resilience under dynamic cyber threats.

Cross Cutting Research Issue:

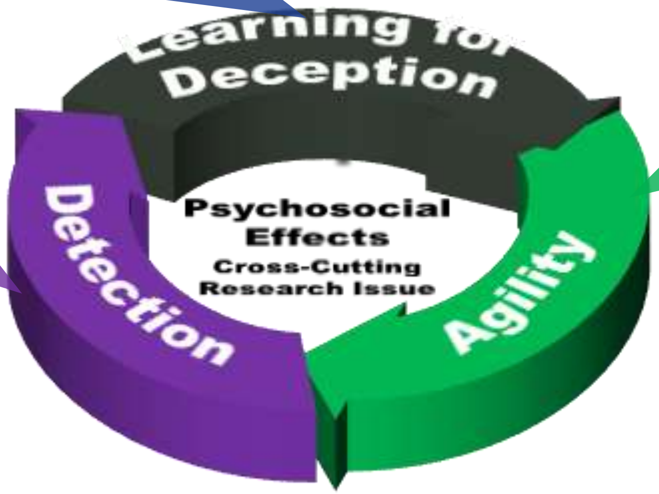
- **Psychosocial Effects:** Theoretical understanding of the socio-cognitive factors that impact the decision making of the user, defender, & adversary

EXPECTED OUTCOMES

Foundational cross-disciplinary research in cyber security, resulting in greatly enhanced cyber threat detection, autonomous planning and control of cyber maneuvers, and adaptive reasoning for deception in complex, adversarial, and uncertain environments at the Army's tactical edge

Adaptive algorithms that reason about adversarial intent, employs deception to protect forces, & defeats enemy AI

Cyber threat detection & recognition in complex, adversarial, & uncertain environments

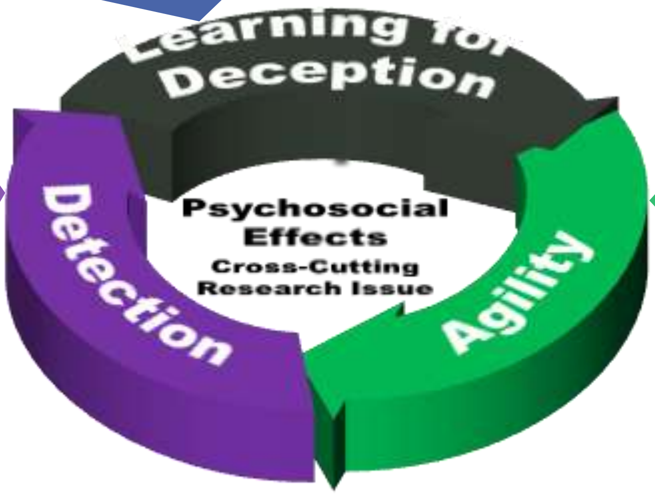


Autonomous planning & control of cyber maneuvers to deceive adversaries & protect networks

RESEARCH TASKS

- **L1:** Adversarial Machine Learning
- **L2:** Learn to Defend Against Unknown Attackers & Deceptive Attacks
- **L3:** Dynamic Honeynets that Adapt to Adversarial Actions

- **D1:** Intelligent Evidence Collection & Cultivation
- **D2:** Scalable Hypothesis-based Detection for Mission Resilience
- **D3:** Robustness to Adversarial Manipulation in Cyber Networks



- **A1:** Multi-Attacker/ Defender Game-Theoretic Models with Insiders & Colluders
- **A2:** Intelligent Networked System Agility
- **A3:** Defending the Dark Triad in Cyber Security Using Game Theory

HBCU/MI Partnered Research Initiative

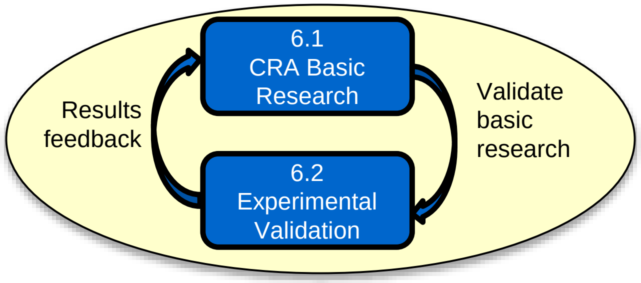
APPLIED RESEARCH & EXPERIMENTATION PARTNER (AREP)

The purpose of AREP is to bridge the cyber security knowledge gap between Army strategic and tactical cyber domains by developing an innovative applied research and experimentation program that can assess the validity of the Cyber CRA basic research while measuring the psychosocial effects on operators.

- Allows for CCDC C5ISR Center and ARL to collaboratively work to ensure successful transition of defensive cyber operations
- Ensure that CCDC C5ISR Center and ARL plan future R&D efforts
    - Jointly developed 30 year cyber research roadmap
    - Quick technology transitions, shaping of large defensive cyber programs, and lessons learned to re-orient ongoing efforts
- Enable access to industry partner to find hard to fill roles for personnel who can successfully move basic to applied research

CYBERVAN TESTBED

- The goals of the AREP (Cyber Security Applied Research and Experimentation Partner) program are:
  - Experimental validation of cyber security research being conducted under the Cyber Security CRA
  - Research into innovative experimental approaches
  - Development of a cyber experimentation testbed



Develop ***relevant*** scenarios

- ***Realistic*** tactical and strategic networks, publicly releasable specs
- ***Relevant*** traffic and configurations

Model cyber effects ***relevant*** to CRA

- Relevant attacks
- Benign background activities
- Relevant data collection
- Enable incorporation of CRA research prototypes

Hybrid emulation testbed: CyberVAN

- Applications run on VMs over simulated network
- Supports large-scale, high-fidelity experimentation

SUMMARY

Develop the theoretical underpinnings for a Science of Cyber Security