



Cyber Security CRA Overview

Patrick McDaniel (PM, PSU) & Edward Colbert (CAM, ARL)

cra.psu.edu

Approved for public release;
distribution is unlimited.



U.S. ARMY
RDECOM

UNCLASSIFIED

**Cyber Security Collaborative
Research Alliance**

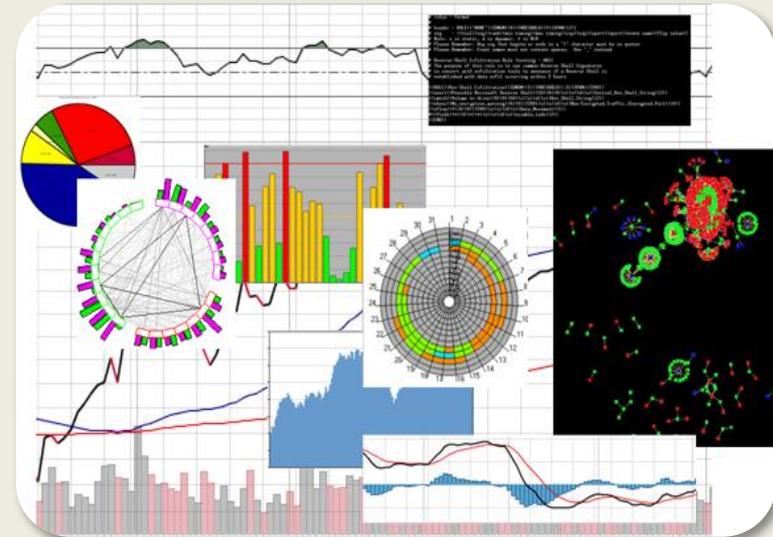
ARL

A Collaborative Alliance between ARL, CERDEC, 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**



UNCLASSIFIED

The Nation's Premier Laboratory for Land Forces



Grand Science Challenges:

- Joint study of inter-related areas of Risk, Detection and Agility
- Understanding human dynamics: defense and attack
- Strategic & tactical networks

Domain

- **Heterogeneous & convergent networks**
- **Army must:**
 - Use & defend networks that it neither owns nor directly controls
 - Construct mission networks with a variety of partners & allies
 - Adapt to rapidly changing technologies, tactics, & threats
 - Maintain situation awareness across complex networks

Army-unique Challenges

- **Large attack surface**
- **Relatively disadvantaged assets**
- **Large scale & high dynamics**
- **Advanced persistent threats**
- **Close proximity with threats**
- **Disadvantaged users**
- **Must work through contested and compromised environments**



Develop an understanding of cyber phenomena:

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

Research Areas

- **Risk:** Theories and models that relate fundamental properties of dynamic risk assessment to the properties of dynamic cyber threats, Army's networks, and defensive mechanisms
- **Detection:** Theories and models that relate properties and capabilities of cyber threat detection and recognition to properties of malicious activity
- **Agility:** Theories and models to support planning and control of cyber maneuver in network characteristics and topologies



Cross Cutting Research Issue

- **Human Dimensions:** Theoretical understanding of the socio-cognitive factors that impact the decision making of the user, defender, and adversary



U.S. ARMY
RDECOM

UNCLASSIFIED

Cyber Security Collaborative Research Alliance



Goal: Develop a rigorous science of cyber-security

RISK

Theories and models of risk assessment in cyber-environments that combine:

- System and network risk
- Human oriented risk

DETECTION

Theories and models of detection that provide:

- What is the most likely threat
- What impact will it have
- The confidence in the process

AGILITY

Theories and models of system agility that reason about:

- The universe of security-compliant maneuvers and end-states
- The impacts of maneuvers on humans and outcomes

Psychosocial Effects: A Cross-Cutting Research Issue

Theories and models of user behavior in cyber-environments:

- Classify user intent and capability
- Predict how a user will react to stimuli
- Induce mitigating adversarial behavior

Operations Model: An Integrating Framework

Formal structures for reasoning about cyber-maneuvers and security goals/ strategies

Mathematical representations that are decomposable and composable in ways that make analysis tractable and answer key questions

PENNSTATE



Carnegie
Mellon
University

INDIANA

UCDAVIS
UNIVERSITY OF CALIFORNIA

UNIVERSITY OF CALIFORNIA
UCRIVERSIDE

APPLIED
COMMUNICATION
SCIENCES

★ CERDEC
US ARMY - RDECOM





OPERATION MODEL

O1: Operation Model Development and Ontology

RISK

R1: Advancing models of risk through Integration of cultural and cognitive individual factors

R2: Integrative Cyber-Security Risk Modeling: Validation, Predictive Modeling, and Experimentation

DETECTION

D1: Science of Evidence Collection

D2: Resilient Detection in Adversarial Settings

AGILITY

A1: Software Maneuvers

A2: Game Theoretic Models to Capture End State Dynamics

A3: Defeating the Dark Triad in Cyber Security Using Game Theory

**Psychosocial Effects:
Cross-Cutting Research Issue**

**Validation / Experimentation:
Cross-Cutting**

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



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.

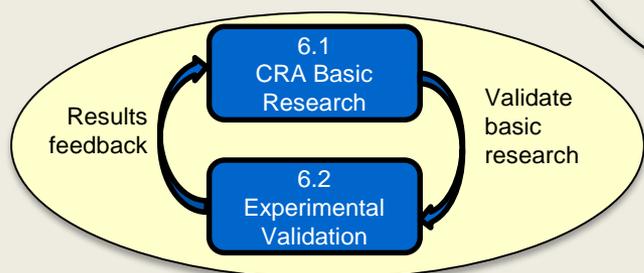
- Allows for ARL and CERDEC to collaboratively work to ensure successful transition of defensive cyber operations
- Ensure that CERDEC and ARL plan future R&D efforts
 - Jointly developed 30 year cyber research roadmap
 - Quick technology transitions, shaping of large defensive cyber programs, and lessons 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





- The goals of the ARL CERDEC 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



Develop the theoretical underpinnings for a Science of Cyber Security

