

Cyber Security Research Alliance

ARL CAM-Ananthram Swami, ananthram.swami.civ@mail.mil

University Lead- Patrick McDaniel, mcdaniel@cse.psu.edu

Objective

The overall objective of the Cyber Security CRA is to develop a fundamental understanding of cyber phenomena, including aspects of human attackers, cyber defenders, and end users, so that fundamental laws, theories, and theoretically grounded and empirically validated models can be applied to a broad range of Army domains, applications, and environments. ARL envisions the alliance bringing together government, industry and academia through this basic research program to develop and advance the state of the art of Cyber Security in the following areas:

- Risk Research Area seeks to develop theories and models that relate fundamental properties and features of dynamic risk assessment algorithms to the fundamental properties of dynamic cyber threats, Army's networks, and defensive mechanisms.
- Detection Research Area seeks to develop theories and models that relate properties and capabilities of cyber threat detection and recognition processes/mechanisms to properties of a malicious activity, and of properties of Army networks.
- Agility Research Area seeks to develop theories and models to support planning and control of cyber maneuver (i.e., "maneuver" in the space of network characteristics and topologies) that would describe how control and end-state of the maneuver are influenced by fundamental properties of threats, such as might be rapidly inferred from limited observations of a new, recently observed threat.

Consortium Members

- Pennsylvania State University (University Lead)
- Carnegie Mellon University
- Indiana University
- The University of California at Davis
- The University of California Riverside

