BACKGROUND
The Army battlefield is quickly becoming a highly converged virtual-physical space, where cyber operations will be an integral part of the fight. Cyber Fires will degrade, disrupt, deny, deceive and destroy informational, computational and communication resources of the adversary, and the physical capabilities of its platforms, weapons, robots and munitions. Cyber maneuver will rapidly move and/or transform, in cyberspace, the friendly informational-computational resources to deny the adversary an opportunity to attack, at a great cost to the adversary. The Cyber Research Center (CRC) provides an opportunity to foster collaboration across ARL, national labs, industry and universities to accelerate innovative solutions for highly agile, daring and aggressive cyber fires and maneuvers.

COLLABORATIVE FOCUS
The CRC provides a collaborative environment for increasing understanding of cyber phenomena, including the interactions of information and information systems with cyber users, defenders and attackers – human and/or intelligent agents.

BENEFITS
The CRC provides a collaborative, creative environment for advancing cyber science on multiple fronts such as:
• Anticipation, detection and identification of threats
• Methods for active response
• Characterization and prediction of risks
• Quantifying effects of cyber maneuvers
• Inferring adversarial intent

UNIQUE FACILITIES
• Army Cyber Research and Analytics Laboratory (ACAL) – cloud computing, product integration & testing, collaboration space
• Cyber Virtual Assured Network (CyberVAN) – experimental cyber test range with remote access to batch cyber simulations, humans-in-the-loop and hardware-in-the-loop experimentation
  • Cyber Security Collaborative Research Alliance – understand cyber phenomena, cyber risk, detection and agility and psychosocial effects

PARTICIPANTS
Open to national and defense labs, universities, and industry.

CONCEPT OF OPERATION
The CRC will utilize CRADAs, MOUs and/or MOAs to define the extent of collaboration under the center, the disposition of intellectual property, and the sharing of research outcomes and laboratory resources.

POINT OF CONTACT
Jerry Clarke
Chief Network Security Branch
301.394.0798
Jerry.a.clarke4.civ@mail.mil