

Opportunity Title: Computationally Intelligent, Assured and Distributed Decision-Support for Cyber Operations

Opportunity Reference Code: ARL-R-CISD-300151

Organization DEVCOM Army Research Laboratory

Reference Code ARL-R-CISD-300151

How to Apply A complete application includes:

- **Curriculum Vitae or Resume**
- **Three References Forms**
 - An email with a link to the reference form will be available in Zintellect to the applicant upon completion of the on-line application. Please send this email to persons you have selected to complete a reference.
 - References should be from persons familiar with your educational and professional qualifications (include your thesis or dissertation advisor, if applicable)
- **Transcripts**
 - Transcript verifying receipt of degree must be submitted with the application. Student/unofficial copy is acceptable

If selected by an advisor the participant will also be required to write a **research proposal** to submit to the ARL-RAP review panel for :

- Research topic should relate to a specific opportunity at ARL (see [Research Areas](#))
- The objective of the research topic should be clear and have a defined outcome
- Explain the direction you plan to pursue
- Include expected period for completing the study
- Include a brief background such as preparation and motivation for the research
- References of published efforts may be used to improve the proposal

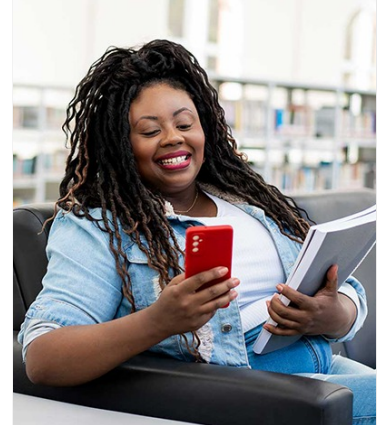
A link to upload the proposal will be provided to the applicant once the advisor has made their selection.

Description About the Research

The next-generation battlefield will be populated with a vast number of interconnected, heterogeneous and sometimes autonomous agents including devices, networks, software, and humans. Defending such complex and/or autonomous systems will be impossible for humans to do alone, making research in this area key in defending such system. The Army Cyber Institute (ACI), United States Military Academy (USMA) at West Point, NY is looking for a Postdoctoral Research Fellow to join the ACI's Data and Decision Sciences research team and work on projects supporting the ACI's Intelligent Cyber-Systems and Analytics Research Lab and the ACI's Internet of Things Research Lab. In response to the ongoing and future challenges facing the Cyber and Information Domain, our projects support the research, development, experimentation, testing, evaluation and operationalization of computationally intelligent, assured (secure, resilient, robust, trusted), and distributed decision-support systems for autonomous cyber operations in highly-contested, complex battlefield



ORA Pathfinder



Whether you are just starting your career or already at a senior level, ORAU offers internships, fellowships, research opportunities, and contract positions that can provide you with invaluable experience. Download the ORAU Pathfinder mobile app and find the right opportunity to propel you along your career path!

Visit ORAU Pathfinder [↗](#)



Opportunity Title: Computationally Intelligent, Assured and Distributed Decision-Support for Cyber Operations

Opportunity Reference Code: ARL-R-CISD-300151

environments. To build, assess and deploy smart, autonomous cyber-systems that enable intelligent, assured and federated decision-making, our research explores the science of information, computation, learning, and fusion for adaptive, collaborative pattern discovery, reasoning, perception, action and decision-making given heterogeneous, complex, disparate data spanning devices, networks, software, and humans. Overall, our research aims to develop models and tools for collective intelligence, likely augmented by interacting with human cyber analysts and decision-makers.

We are looking for a candidate interested in conducting basic and applied research and development with the objective of providing new capabilities to: shift emphasis from sensing to information awareness; understand the underpinning of autonomy; relieve human cognitive overload in dealing with the data deluge problem; enhance human-machine interface in information processing; cope with various complex disparate data/information types; integrate a diversity of unique reasoning and learning components collaborating simultaneously; bridge correlational with causal discovery; determine solutions or obstructions to local-to-global data fusion problems; mechanize reasoning/learning and computing in the same computational environment; yield provably efficient procedures to enable or facilitate advanced data analytics; and deal with high-dimensional and massive datasets with provably guaranteed performance.

Over the fellowship term, the participant will research new generative methods and artificial intelligence model architectures to generate adversarial examples by perturbing entries in network intrusion detection system (NIDS) data while investigating/ considering the constraints on certain cyber data features as they pertain to functionality retention. The participant will research techniques to facilitate and simplify the risk-aware application of reinforcement learning algorithms to applications spanning from C3I decision-support to autonomous cyber defense to automatic sensor optimization. The participant will research theory, principles, and methodologies to make individual machine learning and artificial intelligence models and their integration into operational environments provably-robust and resilient to adversarial attacks. The participant will research fundamental optimization problems focused on robustness and performance while considering distributed and decentralized implementation.

The successful candidate will be expected to take a leading role in developing, testing, and implementing generative machine learning (GML) to the cyber domain and its evolutionary properties. The closed world model of machine learning can fail catastrophically upon encountering the unknown. The successful candidate will explore open world recognition (OWR) for the cyber domain to enable cyber machine learning evolution within a rapidly changing environment. Within the context of the cyber domain, how do we anticipate newly emerging attack vectors and classes of data? How can we have proactive evolution of generated cyber data targeted towards adversarial behavior? The objective of this research will be to investigate and develop GML techniques for out-of-distribution

Opportunity Title: Computationally Intelligent, Assured and Distributed Decision-Support for Cyber Operations

Opportunity Reference Code: ARL-R-CISD-300151

training data expansion in the NIDS setting, to include cyber adversarial behavior evolution. The candidate will aim to generate evolutionary cyber machine learning data sets for OWR, as well as conduct temporal testing for evolution (injecting adversarial evolution through GML, cyber adversarial modeling, and subject-matter-expert input). Evolutionary computation, reinforcement learning, uncertainty quantification, and statistical computing methods will be explored for modeling and simulation to enable broad resilience.

It is expected that the applicant will be able to assist in the writing of scholarly manuscripts along with reimbursable research project white papers and proposals, making positive scholarly contributions that are of mutual interest with the Principal Investigator, and also productively interact with research collaborators within the ACI, across USMA, and with external partners.

ARL Advisor: Nathaniel D. Bastian

ARL Advisor Email: nathaniel.bastian@westpoint.edu

About CISD

The [Computational and Information Sciences Directorate \(CISD\)](#) conducts research in a variety of disciplines relevant to achieving and implementing the so-called digital battlefield. Problems address the sensing, distribution, analysis, and display of information in the modern battle space. CISD research focuses on four major areas: communications, atmospheric modeling, battlefield visualization, and computing

About ARL-RAP

The [Army Research Laboratory Research Associateship Program](#) (ARL-RAP) is designed to significantly increase the involvement of creative and highly trained scientists and engineers from academia and industry in scientific and technical areas of interest and relevance to the Army. Scientists and Engineers at the CCDC Army Research Laboratory (ARL) help shape and execute the Army's program for meeting the challenge of developing technologies that will support Army forces in meeting future operational needs by pursuing scientific research and technological developments in diverse fields such as: applied mathematics, atmospheric characterization, simulation and human modeling, digital/optical signal processing, nanotechnology, material science and technology, multifunctional technology, combustion processes, propulsion and flight physics, communication and networking, and computational and information sciences.

Questions about this opportunity? Please email

ARLFellowship@ora.u.org.

Qualifications The Postdoctoral Research Fellow will conduct work at the Army Cyber Institute, United States Military Academy located at Spellman Hall, 2101 New South Post Road, West Point, New York 10996. The successful

Opportunity Title: Computationally Intelligent, Assured and Distributed Decision-Support for Cyber Operations

Opportunity Reference Code: ARL-R-CISD-300151

candidate should have proficiency in programming languages (Python, R, Julia, Matlab, etc.) along with modern software development practices, tools and technologies. The candidate should have knowledge of computer and network security principles, as well as knowledge of general cybersecurity data sets and tools.

- Eligibility**

Requirements
- **Citizenship:** U.S. Citizen Only
 - **Degree:** Bachelor's Degree, Master's Degree, or Doctoral Degree.
 - **Academic Level(s):** Any academic level.
 - **Discipline(s):**
 - **Computer, Information, and Data Sciences** ([5](#) 👁)
 - **Engineering** ([4](#) 👁)
 - **Mathematics and Statistics** ([3](#) 👁)
 - **Social and Behavioral Sciences** ([1](#) 👁)