Opportunity Title: Robust and Resilient Artificial Intelligence Systems
Opportunity Reference Code: ICPD-2023-21

Organization
Office of the Director of National Intelligence (ODNI)

Reference Code
ICPD-2023-21

How to Apply
Create and release your Profile on Zintellect – Postdoctoral applicants must create an account and complete a profile in the on-line application system. **Please note: your resume/CV may not exceed 2 pages.**

Complete your application – Enter the rest of the information required for the IC Postdoc Program Research Opportunity. The application itself contains detailed instructions for each one of these components: availability, citizenship, transcripts, dissertation abstract, publication and presentation plan, and information about your Research Advisor co-applicant.

Additional information about the IC Postdoctoral Research Fellowship Program is available on the program website located at: https://orise.orau.gov/icpostdoc/index.html.

If you have questions, send an email to ICPostdoc@orau.org. Please include the reference code for this opportunity in your email.

Application Deadline
2/28/2023 6:00:00 PM Eastern Time Zone

Description
Research Topic Description, including Problem Statement:

Over the last decade, Artificial Intelligence (AI) Systems have become more prominent in people's daily lives. Despite their widespread adoption and usage, these AI systems can still be fooled, and therefore are vulnerable to adversarial attack. Such vulnerabilities can lead to severe consequences depending on the system being exploited. For instance, in the case of biometrics systems such as facial or speaker recognition, a bad actor could develop techniques that allow them to evade detection or impersonate another identity to gain access to sensitive data.

With this project the goal is to investigate the various ways machine learning systems, such as face and speaker recognition systems, are vulnerable to adversarial attacks and how these types of systems can be made more robust to these attacks.

Example Approaches:

Researchers have demonstrated various ways in which inputs can be modified in an adversarial manner so that they fool a recognition system. Example techniques include adding imperceptible noise patterns or editing features (e.g., varying the lighting) for computer vision based systems, and the generation of entirely synthetic data instances/Deepfakes for speaker recognition systems. Exploring how to defend against these techniques, and how they can be detected, is an active research area that can be explored.

Relevance to the Intelligence Community (IC):

The rapid spread of deceptive digital content poses a serious threat to maintain a competitive edge in the use of Artificial Intelligence systems. Current methods to detect inauthentic digital content have made significant progress, but synthetic data/Deepfake generation algorithms are continuously evolving, improving their realism and avoiding detection. The work described above would explore detection systems needed to detect and counter highly dynamic false threats.

Qualifications
Postdoc Eligibility

- U.S. citizens only
- Ph.D. in a relevant field must be completed before beginning the appointment and within five years of the application deadline
- Proposal must be associated with an accredited U.S. university, college, or U.S. government laboratory
- Eligible candidates may only receive one award from the IC Postdoctoral Research Fellowship Program

zintellect
climb higher

Opportunity Title: Robust and Resilient Artificial Intelligence Systems
Opportunity Reference Code: ICPD-2023-21

Research Advisor Eligibility

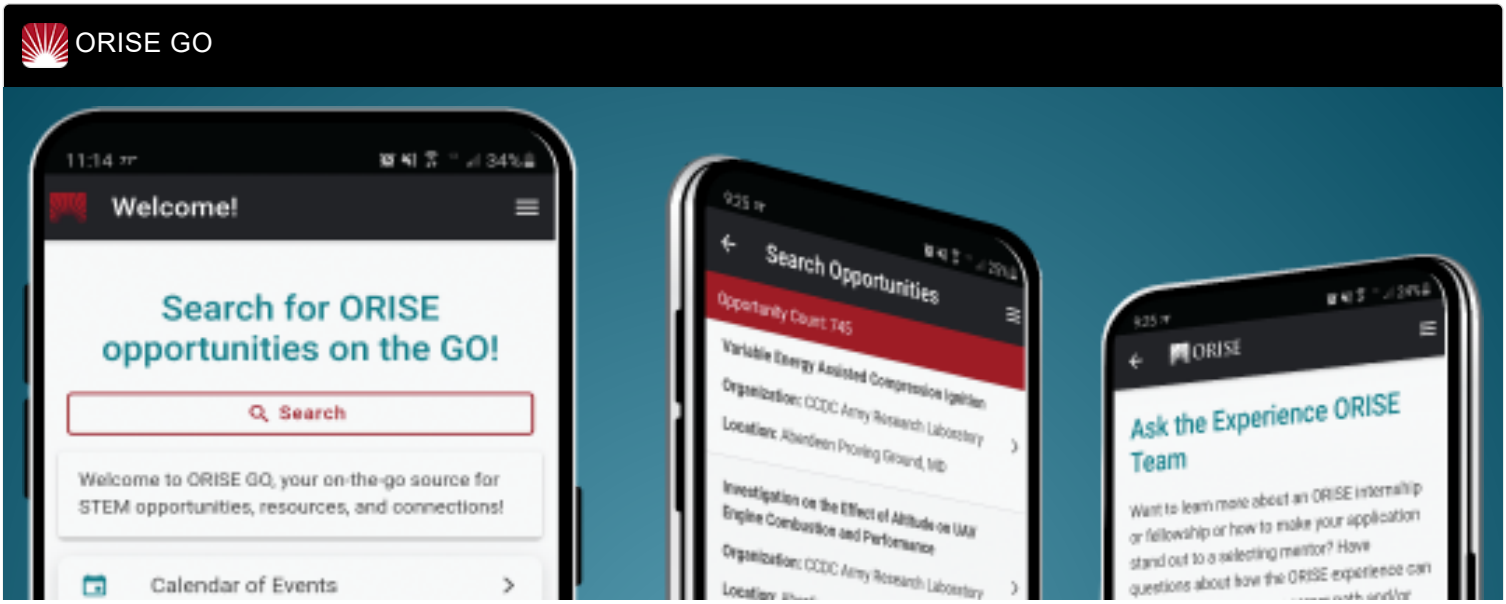
- Must be an employee of an accredited U.S. university, college or U.S. government laboratory
- Are not required to be U.S. citizens

Key Words: #Artificial Intelligence, #AI, #Adversarial Machine Learning, #Biometrics, #Deepfake, #System Robustness, #Face Recognition, #Computer Vision, #Speaker Recognition

Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.
- **Discipline(s):**
  - **Chemistry and Materials Sciences** (12 👁)
  - **Communications and Graphics Design** (6 👁)
  - **Computer, Information, and Data Sciences** (17 👁)
  - **Earth and Geosciences** (21 👁)
  - **Engineering** (27 👁)
  - **Environmental and Marine Sciences** (14 👁)
  - **Life Health and Medical Sciences** (48 👁)
  - **Mathematics and Statistics** (11 👁)
  - **Other Non-Science & Engineering** (2 👁)
  - **Physics** (16 👁)
  - **Science & Engineering-related** (1 👁)
  - **Social and Behavioral Sciences** (29 👁)

OAK RIDGE INSTITUTE FOR SCIENCE AND EDUCATION



Opportunity Title: Robust and Resilient Artificial Intelligence Systems
Opportunity Reference Code: ICPD-2023-21