Opportunity Title: Adversarial biological learning
Opportunity Reference Code: IC-18-09

Organization Office of the Director of National Intelligence (ODNI)

Reference Code IC-18-09

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://orau.org/icpostdoc/.

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

Application Deadline 3/12/2018 11:59:00 PM Eastern Time Zone

Description **Research Topic Description, including Problem Statement:**

- In adversarial machine learning, an artificial neural network (ANN) is trained to classify images (or other data) at a high level of accuracy. An adversarial attack manipulates the image very subtly and causes the ANN to misclassify the image with a high degree of confidence. Is there a biological analogue? Can a normally-accurate biological neural network (BNN) classifier be made to confidently misclassify an image after it is manipulated very subtly? Is the robustness or weakness of BNNs to adversarial attacks specific to image recognition, or does it extend to all modalities?
- The goal of this topic is to examine how BNNs work and determine if they can be manipulated. Are the principles of adversarial attacks on BNNs different from those on ANNs? Can BNNs be made more robust to such attacks? Known adjacent phenomena are optical illusions, confirmation bias, and (more obtusely) camouflage.

Example Approaches:

- While we are open to all approaches, first steps could involve:
  1. Constructing BNNs,
  2. Training them to classify images or other inputs,
  3. Attempting to create methods that can cause the BNN to misclassify,
  4. Inspecting the BNN to see what internal factors or manipulations affect its robustness.

Notably, there are multiple ways to construct these BNNs, including:

- In vitro with neuron cell cultures or slices.
- In silico methods with detailed physiological models of BNNs, to be contrasted with the simpler ANNs currently used in machine learning.

Note: No Human Subject Research is authorized for the IC Postdoctoral Research Fellowship Program.

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.

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

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** (16 👁)
  - **Earth and Geosciences** (21 👁)
  - **Engineering** (27 👁)
  - **Environmental and Marine Sciences** (14 👁)
  - **Life Health and Medical Sciences** (45 👁)
  - **Mathematics and Statistics** (10 👁)
  - **Other Non-Science & Engineering** (5 👁)
  - **Physics** (16 👁)
  - **Science & Engineering-related** (1 👁)
  - **Social and Behavioral Sciences** (28 👁)