Opportunity Title: Towards Antifragility
Opportunity Reference Code: ICPD-2023-43

Organization	Office of the Director of National Intelligence (ODNI)
Reference Code	ICPD-2023-43

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:

Cyber defense is currently based on resilience: matching known attacks with proven defenses. Adaptation and improvement are only possible using human intervention to inject innovation after the fact.

The concept of Antifragility was suggested by Taleb (2012) [1]. This creates the possibility of using machine learning to create self-healing systems within a cycle of continual improvement. Antifragile cyber systems are therefore systems that are sufficiently resilient to survive preliminary attack, can learn from this experience, and can self-improve. In other words, antifragile systems gain in resilience the more that they are attacked. The technology for achieving this does not yet exist, however, recent encouraging developments in robotics could be used to make progress.

Example Approaches:

The main challenge is establishing an AI that has sufficient self-awareness to interpret the attack experience and innovate improved defensive measures to itself. Specifically, the AI will need:

- A model of self (potentially using machine theory of mind) to discriminate the effects of exogenous events from the effects of self-action
- Perception of malicious agency (i.e., the resolving the attacker as an exploiting/harmful agent using percepts gained through interpretation of sensory data)
- Formulation of attack defenses (solving the correspondence problem [2]: transforming actions in the domain of the attacker to responses in the domain of the defender)
- Deploying effective defenses that do not compromise system function or performance unduly
- Resisting deceptive and/or coercive attacking agents

Detailed challenges include:

- Machine perception of behavior – achieving high accuracy in noisy streaming sensory data
- Characterization – representing the nature of cyberattack in a form that is machine actionable
- Machine innovation – this combines expert knowledge for attack analysis, intimate understanding of the system being defended, and the ability to predict the effect (and side effects) of remedies before deployment
- Whole system perspective – self-remedies are not innovated in isolation; the system must be able to model effects beyond its own limits and avoid unintended consequences

Opportunity Title: Towards Antifragility
Opportunity Reference Code: ICPD-2023-43

- Demonstrate the antifragile property in a real system

References:

[1] Nassim Nicholas Taleb (Author), Antifragile: Things that Gain from Disorder, Random House; Illustrated edition (27 Nov. 2012), ISBN-13: 978-1400067824

[2] Nehaniv, C.L. & Dautenhahn, K., The Correspondence Problem in Social Learning: --What Does it Mean for Behaviors to Match Anyway, 2002, Procs of Perspectives on Imitation: from Cognitive Neuroscience to Social Science, http://hdl.handle.net/2299/1790

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

Key Words: Cyber Defense, Antifragility, Cyber Systems, Artificial Intelligence, Machine Learning

Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.
- **Discipline(s):**
  - **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-S&E** (2 👁)
  - **Other Physical Sciences** (12 👁)
  - **Other S&E-Related** (1 👁)
  - **Physics** (16 👁)
  - **Social and Behavioral Sciences** (29 👁)