

Opportunity Title: The Cybersecurity of Complex Adaptive Systems

Opportunity Reference Code: ICPD-2022-43

Organization Office of the Director of National Intelligence (ODNI)

Reference Code ICPD-2022-43

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.ou.edu/icpostdoc/index.html>.

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

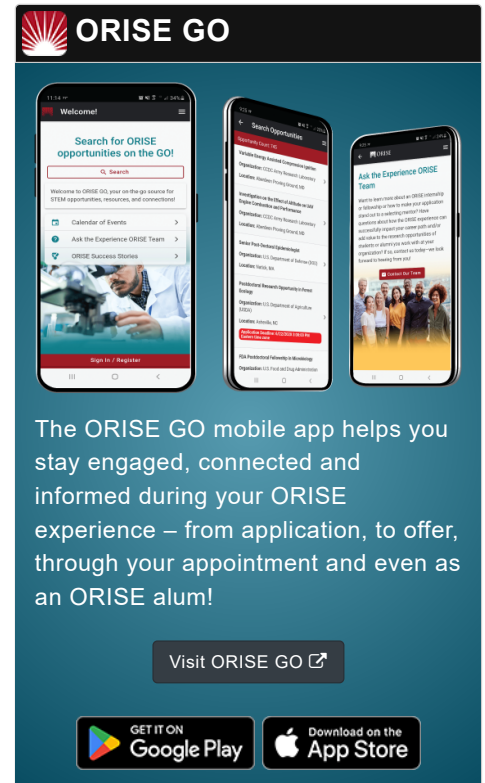
Application Deadline 2/28/2022 6:00:00 PM Eastern Time Zone

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

Sensors/scanners are required by security and defense stakeholders for the detection and identification of threat and prohibited items

As edge computing increases support for AI and machine learning in network devices, we expect future cyber-physical systems to grow in complexity and autonomy, and to work in collectives to achieve the scale required for large-scale cyber-ecosystems (such as in smart buildings, connected places, transport/logistics networks, energy distribution, and other critical national infrastructure). This could result in swarm engineering, or the use of Popperian intelligent agents having an internal model (or representation) of their situation, performance and attainment towards a goal. In either case, there is the potential for new classes of cyber vulnerability based on coercion or deception by an attacker. In addition, we forecast that large-scale collectives of cyber physical systems will increasingly behave as complex systems (CS), or complex adaptive systems (CAS) if learning and/or feedback is present. This too creates new classes of cyber-vulnerability, through the existence of level-points, phase transitions, bifurcation phenomena, percolation phenomena, and other system-wide phenomena new to us. These possibilities therefore need to be understood and prepared for.

A state-based approach has been suggested (Bramson, 2019



[1]) – in which the status and dynamics of the CAS can be represented in the form of a graph.

Figure 1: Graph showing attractor, A1, its basin of attraction (blue), and its support (yellow); and alternative attractor S33 with its basin of attraction (green) (reproduced from Bramson, 2019 [1] p96)

This topic is to establish a theoretical baseline for describing complex adaptive system states and relating this to properties, such as cyber-resilience and antifragility. The challenge includes:

- Representing a CAS in simulation and/or with real data
- Effective identification of CAS system states and the corresponding graph (interdependencies) given that the states are tied to emergent properties, and the system may have been constructed generatively
- Determination of state transition probabilities
- Modelling of high-level phenomena, such as strategic balance points (eg balance between cohesive and exploratory forces), and antifragility
- Relating the state-based model to other representations (such as cyber-physical attack graphs)
- The possibility of metrics (based on probability) for key aspects of system dynamics, such as: Sustainability, Susceptibility, Resilience
- Representing actionable anomaly that is traceable to the actions of an attacker (discriminating endogenous and exogenous sources)
- Identifying prerequisites and design criteria for realistic digital twins representing CAS dynamics

Data will necessarily be synthetic, or restricted domain real-world, for this study as real-world wide area data is not yet available (and probably won't be for some time). We anticipate the need for extensive computer simulation (based on trials and observations) to obtain some of the basic values and identifications. The need for training of key system parameters may require the identification of new machine learning techniques.

Ref: [1] Ted Carmichael (Editor), Andrew J. Collins (Editor), Mirsad Hadžikadic (Editor), Complex Adaptive Systems: Views from the Physical, Natural, and Social Sciences (Understanding Complex Systems), Springer; 1st ed. 2019 edition (27 Jun. 2019), ISBN-13: 978-3030203078

Example Approaches:

Complex System science is a development of General Systems Theory (1968) and some of the principles of Cybernetics (late 1940s), however, it remains immature and incomplete despite this pedigree. Although adequate explanations of Complex

Opportunity Title: The Cybersecurity of Complex Adaptive Systems

Opportunity Reference Code: ICPD-2022-43

Adaptive Systems (CAS) remain elusive, techniques that are available include:

- Hierarchical agent-based modelling underpinned by Markov modelling for explaining CAS behavior
- Generative self-organization using ideas from Finitely Generated Groups
- CAS dynamics using state-based modelling underpinned by Markov modelling
- CAS adaptation using ideas from robotic social learning (with the possibility of achieving antifragile properties)
- Look ahead action modelling and consequence modelling from robotics using evolutionary game theory
- Reflexive control as a potential attack model suitable for representing deception vulnerabilities

A major challenge in dealing with CAS is determining which of the possible approaches to modelling the various characteristics and phenomena are appropriate, and how we can reach a realistic model (even if at low resolution) that is useful.

Relevance to the Intelligence Community:

The IC needs to understand the threats and opportunities from Complex Systems and Complex Adaptive Systems before these architectures are widely deployed.

Key Words: Cybersecurity, Complex

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** (2 )
 - **Computer, Information, and Data Sciences** (16 )
 - **Earth and Geosciences** (21 )
 - **Engineering** (27 )

Opportunity Title: The Cybersecurity of Complex Adaptive Systems

Opportunity Reference Code: ICPD-2022-43

- **Environmental and Marine Sciences** (14 )
- **Life Health and Medical Sciences** (45 )
- **Mathematics and Statistics** (10 )
- **Other Non-Science & Engineering** (2 )
- **Physics** (16 )
- **Science & Engineering-related** (1 )
- **Social and Behavioral Sciences** (27 )