

Opportunity Title: Behavioral Science Tools and Techniques for Identifying and Countering Online Influence Campaigns Fellowship

Opportunity Reference Code: ICPD-2024-31

Organization Office of the Director of National Intelligence (ODNI)

Reference Code ICPD-2024-31

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 3 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.ora.gov/icpostdoc/index.html>.

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

Application Deadline 2/28/2024 6:00:00 PM Eastern Time Zone

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

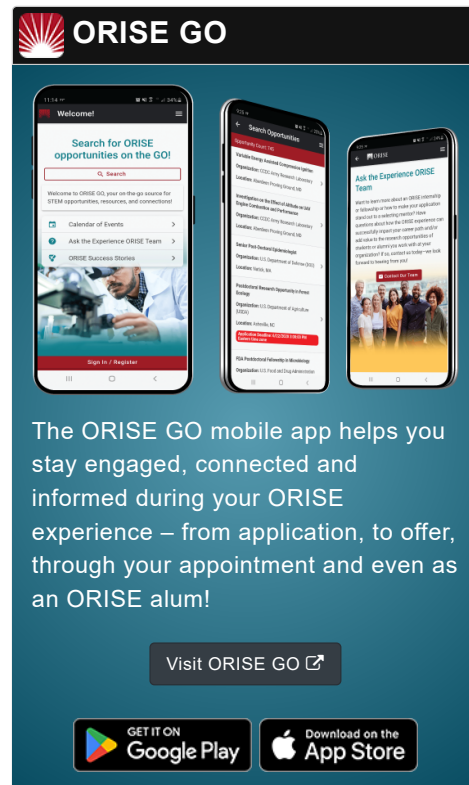
While the online information environment plays an increasingly vital role in social, political and economic activity, at the same time it has become a theatre for “grey zone” activity where influence operations and disinformation campaigns are deployed as tools for coercive statecraft and orchestrated hostile activity.

Well publicized incidents have demonstrated that powerful narratives can be strategically deployed to underpin and sustain attacks on individuals, groups and nations: to misinform, to confuse, to polarize or to disempower. Further, the widespread availability of low-cost computer power coupled with the availability and sophistication of large language models (LLM) and other generative AI capabilities (image/art/meme), mean that the ability to orchestrate and automate influence on an industrial scale is increasingly within reach of small groups and individuals.

Thus, there exists a need to understand how these developments change the way that malicious influence operations can be orchestrated and executed in the online space, both to predict potential malign influence operations, identify threats (and identify threats at speed) and to deploy effective countermeasures.

Problem statement:

- What are the observable indicators that allow us to predict effective vectors of online influence in advance? Such



Opportunity Title: Behavioral Science Tools and Techniques for Identifying and Countering Online Influence Campaigns Fellowship

Opportunity Reference Code: ICPD-2024-31

indicators may include:

- cognitive and meta-cognitive indicators,
 - behavioral indicators, and
 - content-based and narrative features including rhetorical features.
- What are the observable indicators that allow us to detect and quantify the presence of orchestrated online influence? Such indicators may include:
 - cognitive and behavioral indicators,
 - presence of narrative structure in online discourse, and
 - patterns of information flow and social reasoning.
 - Where orchestrated influence is predicted or detected:
 - How can the predicted/detected influence be quantified and visualized so as to highlight strengths, weaknesses, opportunities and threats?
 - Who (individual, group, population) is the influencer?
 - Who is being targeted? And why?
 - Who will be/has been successfully influenced?
 - How can the influence be countered? What are the potential vulnerabilities of the influence campaign?

Example Approaches:

Research proposals could tackle these issues from a variety of perspectives or adopt an integrated trans-disciplinary approach. The problem space intersects with cognitive- and social-psychology (including computational modelling of inference and influence at the individual, group and population level), artificial intelligence (particularly the generative capabilities of LLMs and image/art/meme generation), data science (data assimilation & visualization, and social network analysis), and defense-science (situational awareness, command and control, machine facilitated planning).

Possible lines of investigation might involve:

- Specifying and validating computational models of inference and influence to predict online behavior at the individual, group and population level.
- Using behavioral and data science techniques and capabilities to explore narratives at the macro level in order to understand the influence environment.
- Building analysis pipelines and visualizations to enhance situational awareness.
- Exploiting the generative capabilities of large language models to automate or facilitate the detection and creation of influential narratives.
- Developing algorithms to support machine-facilitated planning and orchestration of counterinfluence campaigns.

Relevance to the Intelligence Community:

While high-profile online influence operations have entered the public consciousness, the full scope of present and future threats

Opportunity Title: Behavioral Science Tools and Techniques for Identifying and Countering Online Influence Campaigns Fellowship

Opportunity Reference Code: ICPD-2024-31

is often unclear. Consequently, when malign influence campaigns do become apparent, a swift response is required. Developing predictive capabilities supports early warning, thereby extending planning lead-time. Enhanced situational awareness supports better identification of strengths, weaknesses, opportunities and threats in contested online spaces. Machine automation and facilitation allows offensive operations to be rapidly planned, monitored and updated. Taken together, these advanced tools and techniques aim to support the intelligence community to more effectively deny, degrade, or disrupt malign influence operations.

Reference:

Josh A. Goldstein, Girish Sastry, Micah Musser, Renee Di Resta, Matthew Gentzel, Katerina Sedova, (2023) 'Generative language models and automated influence operations: Emerging threats and potential mitigations', arXiv:2301.04246 [cs.CY], <https://doi.org/10.48550/arXiv.2301.04246>.

Key Words: Detecting online influence, behavioral science, cognitive psychology, narrative visualization, information operations, counterinfluence, generative AI, large language models.

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 appointment start date
- 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** (3 )
 - **Computer, Information, and Data Sciences** (17 )
 - **Earth and Geosciences** (21 )
 - **Engineering** (27 )
 - **Environmental and Marine Sciences** (14 )
 - **Life Health and Medical Sciences** (45 )

Opportunity Title: Behavioral Science Tools and Techniques for Identifying and
Countering Online Influence Campaigns Fellowship

Opportunity Reference Code: ICPD-2024-31

- **Mathematics and Statistics** (11 )
- **Other Non-Science & Engineering** (2 )
- **Physics** (16 )
- **Science & Engineering-related** (1 )
- **Social and Behavioral Sciences** (30 )