zintellect
climb higher

Opportunity Title: Next Generation Vectors, Adversarial Applications, and Defenses Fellowship
Opportunity Reference Code: ICPD-2024-34

Organization Office of the Director of National Intelligence (ODNI)

Reference Code ICPD-2024-34

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.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 2/28/2024 6:00:00 PM Eastern Time Zone

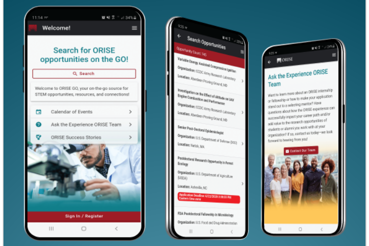
Description **Research Topic Description, including Problem Statement:**

Rapid technical advancements and the convergence of neural hacking and generative AI technologies will likely be adapted to provide adversaries with new and novel vectors for the delivery of mis/disinformation.

Cognitive warfare encompasses activities conducted in synchronization with other instruments of power, to affect attitudes and behaviors by influencing, protecting and/or disrupting individual group cognitions to gain an advantage.[1] The use of weaponized synthetic media (media produced by Generative AI) in cognitive warfare has been widely observed on Western social media platforms; including propaganda about the U.S election in 2016 and recently in the Russian Ukraine conflict.[2]

A Brain Computer Interface (BCI) is “a direct communication pathway between the brains electrical activity and an external device, most commonly a computer or robotic limb” [3] with applications in medical and military domains. Neural hacking refers to identifying and exploiting a weakness in a Brain Computer Interface (BCI) to monitor or manipulate communications for malicious purposes. The US Department of Defense and Defense Advanced Research Projects Agency (DARPA) have invested research into BCI’s. This includes assessing the current and potential Brain Computer Interface (BCI) applications for the military [4] and to develop complex skill learning [5].

Problem Statement:
While we know that research into these new technologies is being explored outside of the medical field, a better understanding of potential risks and implications is required. Understanding the risk posed by these new technologies is critical to developing defensive tools to protect Australia’s national interests. This research project is intended to focus on technology development over the next several years in order to inform and mitigate



risks posed by this fast-developing technology.

Example Approaches:

Research proposals could approach this from a variety of disciplines, or as a cross-disciplinary effort. The problem touches on aspects of psychology, data science, engineering, neuroscience, human-centered computing, systems, and design thinking. Proposals could consider:

- Research into how medical Brain Computer Interface (BCI) and other related technologies could be adapted or manipulated to identify opportunities for or deliver cognitive warfare campaigns and the corresponding defensive mitigations.
- Review global research and development being undertaken and the barriers to entry and utility, including:
    - technical, governance and ethical barriers.
- Understanding the potential of deceptive deployment of non-invasive BCIs.
- Understanding the antecedents to trust BCI technological capabilities that may limit the deployment of these capabilities.
- How may bi-directional BCI’s be manipulated to affect critical decision making or influence a group of individuals.
- Understanding the potential convergence of neural hacking and Generative AI and their application in cognitive warfare.

Relevance to the Intelligence Community:

There have been rapid technological advancements in the applications of these technologies in recent years. The rapidity of developing technologies, and discussions of potential use in conflict situations, indicate that this technology may develop beyond the confines of the medical or other fields. As technologies continue to evolve, it is imperative that the NIC understand the role of new technologies and the implications to inform defensive mitigations. Synthetic media has been identified as a concerning threat to national security as it has been used to undermine the institutional trust and erodes confidence in democratic values.

References:

- 1NATO. (2023) ‘Cognitive Warfare: Strengthing and Defending the Mind. Retrieved from NATO's Strategic Warfare Development Command’, https://www.act.nato.int/article/cognitive-warfare-strengthing-anddefending-the-mind/.
- 2Bushwick, S. (2022) ‘Russia's Information War is Being Waged on Social Media Platforms’, Scientific American, https://www.scientificamerican.com/article/russia-is-having-less-success-at-spreading-socialmedia-disinformation.
- 3’Brain-computer interface’ (2023) Wikipedia, https://en.wikipedia.org/wiki/Brain-computer interface.
- 4Binnendijk, A., Marler, T., & Bartels, M. E, (2020) ‘Brain-Computer Interfaces: U.S Military Applications and Implications, An Intial Assessment’, RAND Corporation, https:///www.rand.org/pubs/research

reports/RR2996.html.
- 5Joeanna Arthur, D. (2019) ‘Targeted Neuroplasticity Training (TNT)’, Retrieved from DARPA.
- Sayler, K. M., & Harris, L. A. (2023) ‘Deep Fakes and National Security’, Congressional Research Service, https://crsreports.congress.gov/product/pdf/IF/IF11333.
- Helmus, T. C. (2022) ‘Artificial Intelligence, Deepfakes and Disinformation. A Primer’, RAND Corporation, https://www.rand.org/pubs/perspectives/PEA1043-1.html.

Key Words: Mis/disinformation information, Cognitive Warfare, Cognitive Domain, Information environment, Neural hacking, Neural networks, Bi-directional Brain Computer Interfaces (BCIs), Generative Artificial Intelligence (AI), Quantum.

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 👁)
    - **Mathematics and Statistics** (10 👁)
    - **Other Non-Science & Engineering** (2 👁)
    - **Physics** (16 👁)
    - **Science & Engineering-related** (1 👁)
    - **Social and Behavioral Sciences** (30 👁)