IDCARE CYBERPSYCHOLOGY RESEARCH PhD SCHOLARSHIPS AND EMPLOYMENT OPPORTUNITIES

www.idcare.org

Background

IDCARE performs a unique role within our community's resilience and response to threats impacting personal, account and credential information. Their work is agnostic to government definitions of threats, whether they be cybercrime, scams or identity theft constructs. The common intersection of IDCARE's work as an international charity is that a person has either been deceived and/or believes that their personal, account, or credential information (including their device) is at future risk of harm.

IDCARE has developed a research program in partnership with the University of Sydney that supports the advancement of new knowledge in the discipline of cyberpsychology and deception. The Cyberpsychology Research Group at the University of Sydney and IDCARE are looking for exceptional applicants that have a passion for understanding the technology and psychology intersections around deception, human behaviours and intervention strategies. To further support suitable applicants, IDCARE is also providing up to 26 hours per week of casual work within its offices adjacent or on-campus depending on local arrangements.

We encourage research applicants that have an interest in undertaking doctoral studies in one of the following related fields:

1. Understanding the psychology of deception and its treatments

There are emerging efforts to better understand deception within an online environment. Research has considered deception and deceptive practices across many disciplines, including computer science, organisational controls, criminology, and more recently cyberpsychology. The latter producing interesting works on 'scam compliance' over the last two decades. Traditional approaches to the study of deception in psychology have focused on visual cues and other non-verbal indicators of lying. The ubiquitous nature of the online environment today, these foundational pieces present opportunities to advance new theories of deception, and critically, an understanding of the psychological impacts of such practice on victims. Put simply, a contemporary development and application of a psychological theory of deception is lacking. With it, comes deficiencies on the most appropriate psychological treatments for victims of scams. Research to date has tended to favour a reliance on experimental research, national crime studies and university participants. An understanding of the psychology of deception and its effects within a clinical setting is largely absent. IDCARE is prioritising this research topic in seeking to support efforts that address one or more of the following questions:

1.1 What are the social, emotional, cognitive and other situational influences on a person's susceptibility to deception?

1.2 How does susceptibility to deception change in relation to a person's identified gender, age, online usage, geographic location, family or other emotional support structures, employment type and status or other socio-demographic attributes if at all?

1.3 What are the short and long-term effects on someone's mental health and well-being after being deceived? Does the nature of the deception and its non-behavioural impacts affect a person's mental health and well-being? Are victims of crimes of deception more prone to presenting indicators of depression and anxiety?

1.4 What are the behavioural treatments for a person that experiences criminal deception? What are they seeking to treat? What treatments have enduring benefits?

1.5 What can response system stakeholders, such as breached organisations, do to prevent and respond to the psychological effects of personal information compromise?

1.6 How does the response to crimes of deception impact a victim's mental health and well-being?

2. Generative AI, deep fakes and at scale deception

With the rapid advancement of Large Language Models (LLMs), there is an inevitability to the deployment by threat actors of generative AI to engage in complex forms of sustained mass misinformation and deception. LLMs are a type of generative AI used to learn and deploy intelligent, adaptive, and knowledgeable text-based communication into the public domain. This cyberpsychology threat is a scale multiplier for intelligent interpersonal deception and political interference. Known as 'Dark LLMs', albeit in their infancy, their targeting will be increasingly aimed at individual cognitive decision-making patterns to influence belief systems, promote maladaptive actions, and defeat sociotechnical controls over long periods. Defending against this threat will require a substantially deeper understanding of deception in a cyberpsychology context where Dark LLMs are deployed and continue to evolve. It warrants an evidence-based approach to reveal the most important social, cognitive, affective, structures and processes leading to deception and maladaptive schema, and their socioeconomic and sociotechnical boundary conditions. This will constitute a paradigm shift in cyber-psychological understanding of mass online deception AI tactics, belief stimuli and response influences as it evolves throughout the research project.

This research priority encourages proposals that focus work in examining one or more of the following questions:

2.1 What is known in the research and grey literatures about the key factors that contribute to computer-mediated deception over time? What are the mediating processes and boundary conditions?

2.2 Can humans tell when they are conversing with an LLM? Can humans tell when they are being deceived by an LLM? What cognitive, demographic, situational and contextual factors affect this?

2.3 What are the most effective and efficient ways to interrupt and disrupt these processes at multiple levels and modalities (e.g., human-to-human target; machine-to-human target, machine-to-machine target levels)?

2.4 How can generative AI (such as LLMs) be used in a scalable way to interdict deception at scale? Can machine-based cognitive support assist in detecting individual LLM deception instances? Are there levels or types of deception, and are some more prone to conventional or LLM delivery?

3. Deceptive acts and their response as a socio-technical system

Socio-technical systems theory recognises that any system is made up of sub-parts that connect people, process, information, and technologies that share in certain assumptions and norms. As a core premises, a socio-technical system shall only evolve effectively and safely if there is alignment and shared understanding of the social and technical aspects that form as interdependent parts of the system. Human factors connect with these theories in striving to make these interdependent parts work more favourably for humans who operate within these complex systems. Deception performed by international organised crime is one form of a complex socio-technical system. These adversaries rely upon many enabling technologies and processes to achieve mass deception at scale. It is obvious to IDCARE when engaging with many thousands of victims that they have been unwitting participants in a much broader socio-technical deception system. Not one cause is often presented as to how a community member has come to be deceived. It is quite often a combination of many actors and elements across the deception sub-systems. This research priority acknowledges the complexity of the socio-technical deception system and encourages researchers to consider the following research questions:

3.1 How are different forms of complex deception better understood through the application of human factors methods?

3.2 Through the application of human factors methods, such as Event Analysis of the Systemic Teamwork, System Theoretic Accident Modelling and Processes, and Accident Modelling, what are the best intervention opportunities that can better detect and respond to complex and at-scale forms of deception?

3.3 How can actors across the deception response system enhance just-in-time interventions and gauge their success through the application of human factors methods?

3.4 By looking at emerging dual use technologies that may enable deception and criminal exploitation of personal information (such as generative AI, neurotechnology, technology automation), what can be discovered through the application of human factors methods in better predicting the risks and anticipating response needs?

Employment Opportunities

IDCARE recognises that PhD candidature is tough and without additional work opportunities can be quite financial constraining. In addition to Scholarship opportunities, for the right candidates, IDCARE will also extend up to 26 hours per week of paid work during their candidature. Work performed will touch upon the many priorities areas performed by IDCARE in responding to crimes of deception impacting community members. It’s a terrific opportunity to provide candidates with a real-world meaningful opportunity to put into practice their research and deliver work outcomes that make a real difference to the lives of many.

Successful candidates that gain employment with IDCARE will be exposed to our National Case Management Centre services as well as other specialist roles within the organisation dependent on a candidate’s suitability, organisational priorities and interests. All candidates will perform some of their time within a Case Management role, growing into a role that provides direct access and support to victims of crimes of deception. At the end of each shift you will know you have made a positive difference to a community member.

Candidates that apply for a PhD scholarship will need to express an interest in IDCARE’s parallel work opportunity. Upon receipt of this expression of interest, a candidate’s details will be shared with IDCARE for independent assessment of suitability under a separate requirement process. For more details about IDCARE please visit idcare.org. You can access the IDCARE Privacy Policy here.