# Developing Cyberpsychology Informed Cyber Deception and Defenses

## BIOGRAPHY

Prashanth Rajivan is an Assistant Professor of Industrial and Systems Engineering at the University of Washington. His research agenda is on the intersection of human factors, simulation modeling and computer security. Prior to this appointment, Prashanth Rajivan was a Postdoctoral Research Fellow at the Department of Social and Decision Sciences, Carnegie Mellon University, Pittsburgh. He holds a Ph.D. in Human Systems Engineering (2014) and M.S. in Computer Science (2011) from Arizona State University, USA. He received the National Science Foundation (NSF) CAREER award in 2022. His work on multi-agent models of teamwork in cyber defense was awarded the best student paper at HFES annual conference in 2014. His dissertation work was a finalist in the Human Factors Prize on Cyber Security in 2017. He was the chair of cyber security technical group at HFES, Co-chair for 2022 USEC (Symposium of Usable Security and Privacy) and was on the board of Modeling and Simulation Society.

## ABSTRACT

Most sophisticated and persistent cyber attacks are primarily human-driven. However, current cyber defenses predominantly focus on technology—patching vulnerabilities or blocking suspicious activities—often neglecting the human element behind these attacks. Few defense and deception methods engage suspected attackers to understand their attributes, skills, or intentions, let alone influence their behavior within the network. This reduces the effectiveness of defense strategies against sophisticated human-driven threats.

Our ongoing work aims to identify cognitive vulnerabilities that attackers may encounter during their workflows and to develop methods that exploit this vulnerability to disrupt their success and increase the odds of detectability. Also, rather than merely detecting and blocking suspicious network activity, we are aiming to develop new defense approaches that increase the effort and resources attsackers must invest by influencing their decision-making. In this talk, I will describe our initial experiments aimed at identifying cognitive vulnerabilities in attackers, present results from these studies, and outline our future approach, including potential solutions and challenges.