Adversarial decision-making could be characterized as decisions made in rare and novel situations, decisions on choices with risky and uncertain outcomes, and decisions made under the adversarial influence. Adversarial decision-making is ubiquitous in cyber security, including the detection of phishing attacks, the detection of misinformation on social networks, the detection of threats in security operations center, and decisions that adversaries make to choose human and computing nodes to attack. We are particularly interested in modeling and analyzing the cognitive processes associated with the operations of human memory in various security contexts to effectively explain adversarial decision making. In this talk, I will describe our work in the context of spear-phishing. First, I will describe a new simulation paradigm we have developed for studying human behavior in phishing attacks from both the attacker and end-user perspective. Next, I will present results of analyzing cognitive model developed to explain and predict human responses to phishing emails obtained from a laboratory experiment. I will describe the effectiveness of integrating natural language processing methods, such as, GloVe, and BERT with cognitive models to predict human response to phishing emails. Finally, I will introduce follow-on research directions I am currently pursuing in the context of misinformation and cyber defense operations.