**Area : Cyber Security**

**Project: Building a secure and trustworthy cyberspace: A behavioral game-theoretic approach**

**Introduction**

Cyber attacks, i.e., the disruption of normal functioning of computers and loss of private information through malicious network cause major work disruption. For example, according to the Indian daily, *Times of India*, Chinese hackers had recently broken into the top secret files of the Indian Defense system (Times, 2010). So far it has been acknowledged that this cyber attack was the biggest security breach in the history of the Indian Defense System (Times, 2010). According to the U.S. Department of Homeland Security's Computer Emergency Readiness Team (CERT), cyber attacks increased almost 40% in 2010. With Anonymous and other threats to corporate and national security, guarding against cyber attacks is becoming a significant part of IT governance, especially because most government agencies and private companies have moved to online systems.

Cyber security is to be studied as a non-cooperative game between attackers and defenders using paradigms based on behavioral game theory and instance-based learning theory. The aim is to determine how a defender’s behavior (experience and tolerance to threats), as well as adversarial behavior (attack strategy), will impact the detection of threats. This program involves studying the influence of motivational factors (e.g., costs and benefits of actions from the attacker’s and defender’s viewpoint), environmental factors (e.g., information available to players about each other), and technology constraints (e.g., how network responds based upon the defender’s actions and network’s accuracy about reporting attacks) on the interaction between attackers and defenders while accountng for cognitive limitations such as the defenders’ and attackers’ memory and recall limitations, and their experiential decisions. This basic research program will help meet our nation’s cyber-security goals.

