# Introduction to the HICSS-56 Minitrack on Cyber Deception and Cyberpsychology for Defense

Kimberly Ferguson-Walter
*Laboratory for Advanced Cybersecurity Research*

Matt Bishop
*University of California Davis*

Cliff Wang
*Army Research Office*

Sunny Fugate
*Naval Information Warfare Center*

This minitrack provides a venue for innovative research that considers the human aspects and limitations of cyber attackers for improved defense within government and other computer networks. Cyber deception techniques are one of the maturing areas of research that focuses on taking advantage of the human limitations and innate performance deficiencies of cyber attackers. Cyberpsychology methods may be used to rigorously quantify the effectiveness of defense methods, provide useful metrics and measures, and understand the decision making and behavioral patterns of cyber attackers or defenders, including insider threats. This information can then be used to help improve defender effectiveness and impede attackers. This minitrack was created to help fill the gap in venues accepting multi-disciplinary work on these topics. The hope is to bring together the different research communities (e.g., computer science, behavioral science, etc.) and experts needed to make significant progress in this area.

This year the minitrack features four papers. These contributions address a range of cyber deception and cyberpsychology research questions that will encourage further exploration of key topics within this domain.

- *"Emotional State Classification and Related Behaviors Among Cyber Attackers"* (by Ryan Gabrys, Anu Venkatesh, Daniel Silva, Mark Bilinski, Maxine Major, Justin Mauger, Daniel Muhleman, Kimberly Ferguson-Walter) demonstrate that an attacker's cognitive and emotional state can often be inferred from data already observed and collected by cyber defenders world-wide.
- *"A Cyber-War Between Bots: Human-Like Attackers are More Challenging for Defenders than Deterministic Attackers"* (by Yinuo Du, Baptiste Prebot, Xiaoli Xi, Cleotilde Gonzalez) propose the design of adversarial human-like cognitive models that are dynamic, adaptable, and have the ability to learn from experience.
- *"Deceptive Self-Attack for Cyber Defense"* (by Jared Chandler, Adam Wick) propose a new cyber-deception technique: deceptive self-attack (DSA) which modifies network and systems to give the appearance that an unknown third party is also at work attacking the same systems.
- *"Accounting for Uncertainty in Deceptive Signaling for Cybersecurity"* (by Edward Cranford, Han-Ching Ou, Cleotilde Gonzalez, Milind Tambe, Christian Lebiere) propose a new algorithm, dubbed Confusion Signaling, that aims to account for uncertainty in an abstracted insider attack scenario.

URI: https://hdl.handle.net/10125/102734
978-0-9981331-6-4