B17 Applied Predictive Behavioral Modeling: The Role of Behavioral Sciences in Digital Forensics

Marcus Rogers, PhD, and Kathryn C. Seigfried-Spellar, PhD*, Purdue University, College of Technology, Knoy Hall of Technology, 401 North Grant Street, West Lafayette, IN 47907*

After attending this presentation, attendees will be familiar with the current state of predictive modeling of cyber adversaries and cyber criminals using behavioral indicators and personality risk likelihood models. It will also provide those interested with a procedure and method to further this type of research.

This presentation will impact the forensic science community by providing understanding of the role that behavioral models can play in predicting adversarial behavior; digital forensics will be better able to take advantage of discoveries and tools from the other forensic sciences. It is also important policy decisions and responses are based on valid real world empirical evidence and not solely on theoretical abstract models that lack any real world credibility.

It has become obvious that purely technical solutions to try and deal with cyber adversaries in a *post hoc* fashion have failed. Business and governments spend more money on cyber security than ever before, yet, if the most recent surveys are believed, the rate of cyber crime and other adversarial attacks is at an all time high. With the current economic crisis budgets are tight and as such it has become increasingly important that any technology expenditures be judged on their Return on Investment (ROI). This shift to an economic model has highlighted that technology alone will not mitigate the risk of cyber crime or cyber attacks.

The fields of predictive analysis and behavioral predictive modeling are now being applied to cyber security and cyber crime space. Several models have developed that, while appearing to be valid from an internal consistency approach, have failed when tested in real world settings. Most of these failed models rely on synthetic data sets, have improper factor loading and issues related to multicolinearity. Even more disturbing is the fact that these failed models are being used to inform government policy and to draft anticipated responses to cyber related events. A further disturbing finding is that in most cases the models were developed with little or no input from behavioral scientists and were based on the fallacy of game theory and behavioral economic: that people are logical rational actors. Human behavior is far more complex than envisioned in these rudimentary models and is more similar to the problem set used for Chaos theory namely irrational behavior.

The current project provides a meta-analysis of behavioral predictive analysis from the areas of insider threat modeling, hacker profiling and cyber terrorism/infowar. The research project focuses on a specific category of cyber criminal behavior (child pornography) and using real world data sets from law enforcement, tested various models to determine their goodness of fit and predictive validity. The Rogers-Seigfried (RS) predictive model was then tested against the same data sets to determine its fit and validity (research ongoing at time of submission)

The results of this research will be presented as well as suggestions for its investigative use and further development of the RS model. The meta-analytic procedure used in the study will also be discussed in order for other researchers to conduct similar studies.

Cyber Crime, Behavioral, Predictive Modeling

 ** Presenting Author*