



Cognitive Foundations of Cyber Analysts



S&T Campaign: Information Sciences Cybersecurity

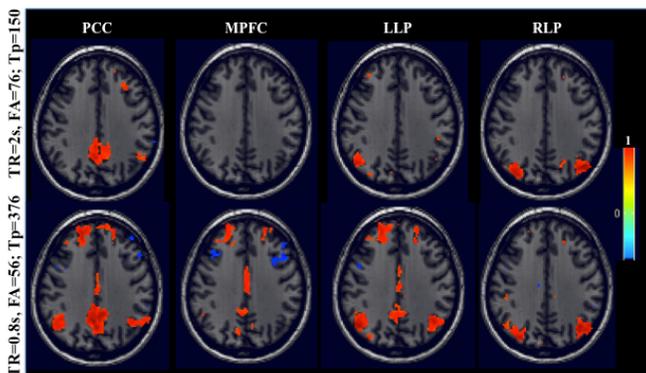
Dr. Robert F. Erbacher, (301) 394-1674
Robert.F.Erbacher.civ@mail.mil

Research Objective

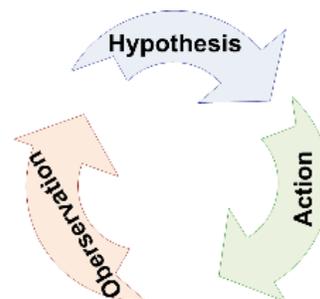
- Quantitatively compare the performance of expert cyber analysts with a baseline tabular display and two alternative displays
- Measure the effectiveness of students as surrogates for expert cyber analysts in user studies
- Develop cognitive models of expert cyber analysts and users to foster the development of new, more effective and cognitively efficient, techniques and capabilities

ARL Facilities and Capabilities Available to Support Collaborative Research

- Leverage ARL's Computer Network Defense Service Provider, i.e., expert analysts and real-world data
- Novel AOH model to aid analysis of process models
 - Zhong et al., "RankAOH: Context-driven similarity-based retrieval of experiences in cyber analysis," CogSIMA, pp.230,236, 3-6 March 2014.
 - Yen et al., "Systematic Capture of Cognitive Reasoning Process of Cyber Analyst Toward Agile Cyber Defense" Springer Cyber Defense and Situational Awareness.
- Unique ARL and related displays
- T Tests: surrogates perform poorer than experts; parallel coordinates perform poorest; node-link display performed nominally better but completed tasks 22+% faster



fMRI studies will aid analysis of cognitive load, impact of learning styles, and identification of characteristics correlated with increased effectiveness



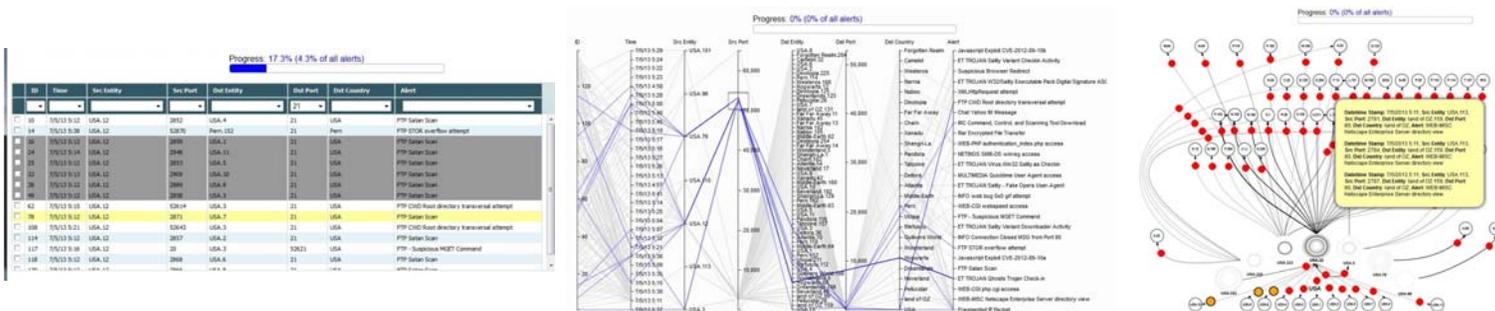
AOH model employed to aid analysis of analyst process models

Challenges

- Unavailability of real-world data and expert cyber analysts on which to perform quantitative user studies and limited knowledge of analyst needs, biases, and processes. This is exacerbated by the need for a significant number of subjects for a valid quantitative user study
- Lack of empirical evidence that alternative displays are effective
- Lack of empirical evidence that students are effective surrogates for expert cyber analysts

Complementary Expertise/ Facilities/ Capabilities Sought in Collaboration

- Comparative analysis with subjects of varying expertise
- Development of models of users
- Comparative analysis of models of experts across domains
- Quantitative study across the breadth of VizSec displays
- Novel analysis and process model paradigms to increase the depth and sophistication of the models and derived understanding from user studies



Baseline tabular display and alternative displays, parallel coordinates and node-link.