Human
Factors
and
Ergonomics
Society

HFES Comments on Human Factors Research Needs Relevant to National Security

February 15, 2017

On behalf of the Human Factors and Ergonomics Society (HFES), thank you for the opportunity to provide input to the National Academies of Sciences, Engineering, and Medicine on the development of a decadal survey on the social and behavioral sciences (SBS) in areas relevant to national security. Outlined below are key challenges facing the intelligence community based on how humans interact with technology.

Continuing advances in technology are leading to new discoveries, practices, and solutions for a wide range of technical, societal, and economic issues. However, successful deployment is strongly dependent on how humans interact with those new technologies. The study of human factors and ergonomics (HF/E) works to develop safe, effective, and practical human use of technology, particularly by developing scientific approaches for understanding the ways in which humans interact with complex systems, known as “human-systems integration.”

A number of emerging issues should be addressed in the upcoming decadal survey on needs for National Security.

(1) Integration of intelligence information and use of big data

Big data analytics are increasingly being used to integrate information across the intelligence community. These techniques have promise, however, they must be used in conjunction with suitable methods for integration with human analysts. This goal can only be accomplished through an understanding of how people process and utilize information in their decision-making activities. Significant research has been conducted on integrating human decision makers with various types of autonomous systems including information fusion and decision support systems (see Endsley, 2017 for a review). Additional research is needed to overcome the significant challenges associated with presentation of information to support understanding the reliability of information (particularly fused data products), calibration of trust in intelligence products, and support for situation awareness of large quantities of data. A challenge for future visualizations is to overcome the bottleneck created by non-standardized, non-integrated and non-interoperable tools that currently permeate the intelligence community.

Endsley, M. R. (2017). From here to autonomy: Lessons learned from human-automation research. Human Factors, 59(1), 116-133.

(2) Autonomy and Risk Assessment and Mitigation

Systemic risk is inherent with increasingly autonomous technology. The increased use of system autonomy introduces new risks including the over reliance of individuals on automated system as well as new risks associated with its interaction with other autonomous systems. Can autonomy be crafted so that when it acts as a force multiplier it does not also act as a risk multiplier in the same or greater proportion? Addressing this issue could draw on the work of economists and experiences with financial instruments that were designed to mitigate risk, but actually exacerbated risk in the edge cases not anticipated by their designers. These risks might be modeled by collective behavior seen in financial markets.

(3) Cyber security and Cyber SA

The United States is highly dependent on computerized systems across civilian, commercial, government and military infrastructures. This dependency creates a significant opportunity for cyber attacks in the form of spamming, spoofing, sabotage and stealing of data. Many cyber security attacks begin with a human vector through known scams (e.g. pfishing, honeypots, etc…). Current firewall and personal security approaches have been fairly unreliable and significantly slow down productivity in most organizations. Research is needed to reduce human vulnerability to cyber attacks, and to improve detection of cyber attacks and cyber situation awareness in intelligence operations. This includes (a) high performance visualization and analytic tools to enhance situational awareness, accelerate threat discovery, and empower task performance, (b)

Autonomy appropriately distributed between operators and machines, enabled by increased transparency of autonomy and increased human “on the loop” or supervisory control, and c) Research to determine the most effective defensive cyber training and the most effective delivery techniques.

(4) Resilience to Information Attack

Recent events have shown that foreign nations can have a significant effect on domestic and government operations through information attacks across distributed decision makers via fake news and widespread dissemination on social networks. Obvious approaches such as discrediting the story can backfire, however, often serving to reinforce it instead. Known decision biases such as anchoring, confirmation bias, and cognitive dissonance exacerbate this problem. Research is needed to determine the best way to detect false information and reduce its effect on naïve decision makers via information presentation, communications, training or other methods.

(5) Human Roles and Interfaces in Adaptive, Learning Systems

Human roles and interfaces are well understood in traditional systems where hardware and software perform known and predictable functions in a mission context. Operator performance and effectiveness are also predictable for these systems during their development. With the emergence of adaptive and learning systems, the determination of the most effective roles and interfaces for human operators becomes problematic because system functionality is not predictable. Research is needed to: (a) determine methods to analyze adaptive, learning systems and define the most effective human roles and interfaces (b) determine effective methods for human operators to adapt to their changing roles as systems learn new ways to cope with new environments, and (c) determine methods of predicting human behavior in adaptive, learning systems where new mission environments may engender unpredicted and possibly rapid responses and function re-allocation.

As background, HFES is a multidisciplinary professional association with 4,500 individual members worldwide, including psychologists and other scientists, engineers, and designers, all with a common interest in creating safe and effective products, equipment, and systems that maximize and are adapted to human capabilities. HF/E works to develop safe, effective, and practical human use of technology, particularly in challenging settings. HF/E experts, research, and perspectives are vital additions to the development of cyber-physical systems.

Thank you for the opportunity to provide comments. Please do not hesitate to contact HFES should you require additional information.

Contact: Mica Endsley
Chair, HFES Government Relations Committee
President, SA Technologies. Inc.
480-386-5200 (office)
mica@satechnologies.com