SAND2013-6404C

Human Dimension in Cyber Operations: Research and Development Priorities

Chris Forsythe, Austin Silva, Susan Stevens-Adams
Sandia National Laboratories

Jeffrey Bradshaw
Institute for Human and Machine Cognition

Address correspondence to
jcforsy@sandia.gov

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Findings from Human Dimension in Cyber Operations workshop

- Workshop was sponsored by Sandia National Laboratories and conducted August 28-29 in Washington DC
- Objectives
  - Explore a range of perspectives regarding the human dimension in cyber operations, with emphasis on the cyber defender;
  - Identify key research and development questions;
  - Establish a community of practice that brings together cyber operations, human factors and S&T leadership;
  - Lay the groundwork for coordinated multi-agency efforts to enhance human effectiveness in cyber operations.
- 32 participants
  - 13 U.S. government organizations, including 9 program managers
  - Backgrounds of participants involved:
    - Operational cyber defense
    - Human factors
    - Government R&D program development and management

What is the problem?

- Cyber defender is asymmetrically disadvantaged faced off against a continually evolving opponent who can attack anywhere, anytime.
- The boundaries of the battlespace are ill-defined, both temporally and spatially.
- Ground truth regarding the attacker, what they've done and how they've done it is rarely known with certainty.
- Any solution must function within the context of an overall system that includes a broad range of users and may span organizational boundaries.
- There are no real measures of success, or progress, rendering the domain an art, precluding the science that might otherwise provide a basis for engineering systems solutions.

Three pillars of a coordinated, integrated research agenda

- Pillar 1: Human factors analysis and scientific studies to establish foundational knowledge concerning factors underlying the performance of cyber defenders.
  - The roles of defenders, users, adversaries, policy makers and the public, including representative use cases.
  - The different jobs and functions within cyber defender teams and the associated knowledge, skills and abilities needed to fulfill these functions.
  - Cognitive processes involved in typical tasks and associated measures of performance both as a basis for selection, and training and operational performance assessment.
  - Methods and materials for training to both requisite levels of performance, as well as a progression from proficient to expert, and potentially elite performer.
  - Allocation of functions between humans and machines, including opportunities to augment human performance through specific technological developments.

Three tiers of a coordinated, integrated research agenda (cont.)

- Pillar 2: Models that capture key processes that mediate interactions between defenders, users, adversaries and the public.
  - Provide sufficient complexity to enable experimentation concerning alternative tactics, techniques and policies.
  - Accommodate insertion of alternative technologies, enabling estimates of the relative returns on investment.
- Pillar 3: Multi-purpose test environment for conducting controlled experiments that enable systems and human performance measurement.
  - Test environment should be flexible to accommodate a range of threats, software tools, modes of training, and policies, as well as mechanisms to simulate users, including the public.

Conclusion