SAND2012-7047P

Human Dimension in Cyber Operations Research and Development Priorities Workshop

August 28-29, 2012

Washington DC

Organized by Sandia National Laboratories

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.

This event is UNCLASSIFIED.

All discussions should be acceptable for Unlimited Public Release.

Classified discussions are NOT permissible in this facility.

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

Agenda

The times listed are approximate and will be adjusted to accommodate progress on assignments and the need to take lunch and other breaks.

Tuesday 28 August – 8:30-4:30

- 8:00 to 8:30 Arrive
- 8:30 to 8:45
  Workshop Objectives
- 8:45 to 11:45
  Perspectives Briefs
- 11:45 to 12:00
  Workshop Process
- 12:00 to 2:30
  Topic 1: What is the problem?
- 2:30 to 4:30
  Topic 2: How might the problem be addressed?

Wednesday 29 August – 8:30-4:30

- 8:00 to 8:30 Arrive
- 8:30 to 9:45
  Topic 3: What can cyber leverage from other domains?
- 9:45 to 11:00
  Topic 4: What are the key research questions?
- 11:00 to 2:30
  Topic 5: What is the strategy for prioritizing research questions?
- 2:30 to 4:30
  Topic 6: How to propose R&D addressing the human dimension in cyber operations?

Perspectives

- Chris Forsythe
- Myriam Abramson
- Ben Apple
- Susanne Bahr
- Phil Bennett
- Ami Bolton
- Jeff Bradshaw
- Marco Carvalho
- Ben Cook
- Nancy Cooke
- Jeremy Epstein
- Kevin Farrell
- Kristin Glass
- Ben Knott
- Mike Lilienthal
- Darren Lynch
- Julie Marble
- Ranjeev Mittu
- Peter Muhlberger
- Kevin Nauer
- Chris North
- Kelvin Oie
- James Patrey
- Perry Pederson
- Gabe Radvansky
- Stephen Russell
- Greg Shannon
- Austin Silva
- Ben Sims
- Tom Starai
- Susan Stevens-Adams
- Ed Talbot
- Rachel Wilson
- Pam Savage-Knepshield
- William Russell

Teams

Team Lead: Susan Stevens-Adams
- Myriam Abramson
- Nancy Cooke
- Darren Lynch
- Peter Muhlberger
- Perry Pederson
- Pam Savage-Knepshield
- Rachel Wilson
- Marco Carvalho

Team Lead: Phil Bennett
- Ben Apple
- Jeremy Epstein
- Julie Marble
- Kevin Nauer
- Gabe Radvansky
- Stephen Russell
- Ed Talbot

Team Lead: Jeff Bradshaw
- Ami Bolton
- Kevin Farrell
- Ranjeev Mittu
- Chris North
- William Russell
- Ben Sims
- Susanne Bahr
- Kristin Glass

Team Lead: Ben Cook
- Ben Knott
- Mike Lilienthal
- Kelvin Oie
- James Patrey
- Greg Shannon
- Austin Silva
- Tom Starai

Topic 1: What is the problem?

How do technologies, systems, organizations and cultures hinder the ability of cyber defenders to be fully effective and accomplish their mission?

- should not be site/domain-specific
- should not be technology(ies)-specific

Outcome: Prepare a 60 second synopsis of the problem – imagine that have 60 seconds to convince a key decision maker who does not appreciate the human dimension and is being encouraged to prioritize other research investments.

Topic 2: How might the problem be addressed?

Please make the following assumption:

> There is no single "magic bullet," but instead, the problem must be addressed through a multi-faceted, systems-level solution.

What are the elements of a systems-level approach for addressing the human dimension in cyber operations.

Outcome: Prepare a diagram that identifies the elements and the interdependencies between elements of a systems-level solution.

Topic 3: What can cyber leverage from other domains?

What problems involving the human dimension in other domains are analogous to problems posed by cyber operations?

- Identify instances of failures/accidents for which an analogous situation could occur in cyber.
- Identify success stories involving effective interventions that are relevant to cyber.

Outcome: Re-draw diagram from previous exercise to emphasize how elements in the diagram relate to both failure/accident and success stories identified within other domains.

Topic 4: What are the key research questions?

Refer to systems diagram and ask, “What do we need to know that we do not now know to implement the systems solution?”

- 1st Pass – Generate as many research questions as can imagine
- 2nd Pass – Group research questions to form categories reflecting general topical areas

Outcome: Prepare a presentation that discusses each topical area and provides one or more examples of specific research questions from each topical area.

Topic 5: What is the strategy for prioritizing research questions?

Transition from putting things on the table to potentially taking things off the table.

1st Pass – Using research topics from previous exercise, imagine that have 10 funding tokens to distribute across the research topics. How do you distribute your 10 tokens?

2nd Pass – Describe the strategy used for distributing tokens.

Outcome: Prepare a presentation discussing the strategy for distributing funding tokens, including the assumptions, motives and other factors embodied by your strategy.

Topic 6: How to propose R&D addressing the human dimension in cyber operations?

Imagine you are one of several program managers competing to obtain funding for a new program of research and development.

- Assume there are sufficient funds available for a large-scale, multi-year program to develop a comprehensive solution.
- Address only the technical elements – do not worry about $'s, years and administrative details.

Outcome: Prepare a five minute, oral program proposal that addresses:

(1) What is the problem and why it is hard?
(2) What are the limits of current practice?
(3) What are the objectives and what difference will it make?
(4) How will you measure success/progress?