Human Dimension in Cyber Operations Research and Development Priorities

Chris Forsythe[a], Austin Silva[a], Susan Stevens-Adams[a], Jeffrey Bradshaw[b]

[a] Sandia National Laboratories, Albuquerque, NM, USA, [b] Institute for Human and Machine Cognition, Pensacola, FL, USA
jcforsy@sandia.gov, aussilv@sandia.gov, smsteve@sandia.gov, jbradshaw@ihmc.us

Abstract. Within cyber security, the human element represents one of the greatest untapped opportunities for increasing the effectiveness of network defenses. However, there has been little research to understand the human dimension in cyber operations. To better understand the needs and priorities for research and development to address these issues, a workshop was conducted August 28-29, 2012 in Washington DC. A synthesis was developed that captured the key issues and associated research questions. Research and development needs were identified that fell into three parallel paths: (1) human factors analysis and scientific studies to establish foundational knowledge concerning factors underlying the performance of cyber defenders; (2) development of models that capture key processes that mediate interactions between defenders, users, adversaries and the public; and (3) development of a multi-purpose test environment for conducting controlled experiments that enables systems and human performance measurement.

1 Introduction

Within cyber security, the human element represents one of the greatest untapped opportunities for increasing the effectiveness of network defenses. However, there has been little research to understand the human dimension in cyber operations. To better understand the needs and priorities for research and development to address these issues, a workshop was conducted August 28-29, 2012 in Washington DC. The findings of the workshop are summarized in this report.

The workshop brought together operational, scientific and programmatic perspectives, with the objective to converge upon a prioritized list of key research questions. While the human dimension encompasses defenders, attackers and users, for the current workshop, emphasis was focused only upon defenders. A range of topics were considered that contribute to increasing the effectiveness of cyber defenders, while minimizing the impact on users.

The workshop consisted of a series of focused discussions. The scope encompassed all areas impacting the effectiveness of cyber defenders in accomplishing their

adfa, p. 1, 2011.

mission. This included (1) understanding the cognitive processes, (2) application of technology to support and enhance cognitive performance, (3) work processes/environment and other factors that mediate performance, (4) collaboration and teamwork, (5) education and training, (6) organizational and cultural factors, and (7) personnel selection and retention.

2 What are the Key Research Questions?

Research questions were identified that fell into several somewhat overlapping categories. The following sections discuss the core issues underlying these categories.

Measurement and Metrics. For the most part, there currently exists no quantitative basis for assessing the performance of cyber defenders, whether at the individual, team, group or organizational levels. Furthermore, while various resources are available for generating simulated cyber events and observing the behavior and performance of cyber defenders, without underlying science regarding the human dimension within cyber and the associated phenomenology, there is little basis for making decisions concerning the specific nature of exercises, who participates and how performance is evaluated.

Human Performance of Cyber Defenders. From a scientific perspective, there is very little known about cyber analysts. As a basis for scientific study, there is need for analysis to understand the jobs filled by cyber analysts, and particularly, the associated cognitive processes that mediate their performance.

Understanding the Adversary. It may be generally assumed that there is benefit for the cyber defender to have an understanding of their adversary. However, there is need for research to understand what types of knowledge is beneficial and how that knowledge may be effectively put into use.

Selection and Training of Cyber Defenders. Currently, there is little known about what attributes prepare an individual to become an effective cyber defender. There is little understanding of what skills, knowledge and abilities need to be addressed through selection and training. Likewise, within the course of training, there is need for research to scientifically establish the appropriate measures for assessing performance, as well as approaches for effectively diagnosing and intervening to maximize training effectiveness.

Intersection between Humans and Technology. Building upon a better understanding of cyber defenders, questions arise concerning the balance between humans and technology, and how technology may be employed to augment the performance of individuals and teams. These questions generally fall into two related areas. First, which cognitive processes operating at either the individual or team level should technology be used to augment and what mechanisms might be employed to do so.

Second, what technologies would be most beneficial to the cyber defender (e.g. data mining, anomaly detection) and for these technologies, how should they be implemented?

Teamwork and Collaboration. Cyber defense often requires the effective coordination of teams. However, there is little understanding of how teams of cyber defenders operate, and what team processes and communications lead to more effective team performance. Likewise, research is needed that addresses the composition of teams and particularly, provides insight into what kinds of people are needed and how to best cope with situations where highly talented individuals are disinclined and lack the skills needed to operate in a team context.

3 R&D addressing the human dimension in cyber operations

Workshop participants were divided into four groups who developed somewhat overlapping research proposals. The products of the four groups have been integrated to emphasize those points where there was a common appraisal of the problem and the corresponding research questions.

3.1 What is the problem and why is it hard?

Today, the cyber defender is placed in an untenable position. They are 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. In the absence of ground truth, 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.

3.2 What are the limits of current practice?

Today, extensive investments are being made ad hoc to develop software tools that are intended to help cyber defenders. Actions being taken are largely short-term and reactive to known threats. There exists a relatively small pool of qualified professionals with the assignment of personnel to cyber positions often driven more by expediency than thoughtful selection. Current measures provide little insight into the human dimension making it difficult to assess performance, much less draw conclusions regarding what is and what is not working, or the differential contribution of various factors to individual, team or organizational success. Using the tools available to them today, cyber defenders must process large volumes of high-tempo data with it uncertain that this is the right data or that the data is being used in the right way, given that we do not have a good understanding of the actual work being done.

Finally, there has been an insufficient allocation of resources to enable long-term strategic solutions that may require structural and organizational change.

3.3 What are the objectives and what difference will it make?

A coordinated R&D program is needed to accomplish three separate objectives.

The first objective is to conduct human factors analysis and scientific studies to establish foundational knowledge concerning factors underlying the performance of cyber defenders. These studies should address a range of pertinent issues that include:

- The roles of defenders, users, adversaries, policy makers and the public, providing an extensible collection of 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.

The second objective involves the development of models that capture key processes that mediate interactions between defenders, users, adversaries and the public. Models should provide sufficient complexity to enable experimentation concerning alternative tactics, techniques and policies. Models should also accommodate insertion of alternative technologies, enabling estimates of the relative returns on investment.

The third objective is to develop a multi-purpose test environment for conducting controlled experiments that enables systems and human performance measurement. The 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.

Through accomplishing these objectives, cyber operations may be transformed from an art to a science, and based on that science, systems solutions may be engineered to address a range of situations. Likewise, there is an opportunity to move beyond the current state where key decisions (e.g. personnel assignment) are made on a largely ad hoc basis to a state in which there exist institutionalized processes for assuring the right people are doing the right jobs in the right way. These developments lay the groundwork for emergence of a professional class of cyber defenders with defined roles and career progressions, with higher levels of personnel commitment and retention. Finally, operationally, the impact should be evident in improved performance, but also a transition to a more proactive response in which defenders have the capacity to exert some measure of control over the battlespace.

3.4 What are the measures of success/progress?

The first measure of success will be an ability, which does not exist today, to actually measure success. Given the primary product will be knowledge, a second measure of success will be the adoption and institutionalization of the resulting knowledge in establishing selection criteria, measures of performance, training requirements, system specifications for technology products and other related applications. A third measure of success will be the utility attributed to models and resources for conducting testing as evidenced by the amount and diversity of their use.

4 Conclusion

This paper outlines the need for R&D to address the human dimension in cyber operations. The objective of the workshop was to collect a broad set of perspectives and synthesize those perspectives in a form that may be used by different organizations to develop R&D programs. Based upon this exercise, organizations may craft their own proposals having the benefit of knowing how other organizations view the problem and imagine the solutions. It is the intent that this broader awareness will facilitate a more coordinated effort across government organizations than would occur otherwise.

There is a rich collection of experiences in which different domains have taken concrete measures to address the human dimension within their operations. These experiences encompass both engineering analysis, scientific study and the development of technologies, practices, design guidelines and other related products. Cyber is a relatively new domain and recognition of the human dimension in cyber operations is only now rising to the forefront. While cyber does not enjoy the wealth of knowledge and experience that is present with other domains, there is the opportunity for cyber to leverage the knowledge and experiences of these other domains to take similarly effective measures.

5 Acknowledgement

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.