SANDIA REPORT
SAND 2012-9188
Unlimited Release
Printed November 2012

Human Dimensions in Cyber Operations Research and Development Priorities

Chris Forsythe, Austin Silva, Susan M. Stevens-Adams & Jeffrey Bradshaw

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

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.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

Sandia National Laboratories

SAND 2012-9188
Unlimited Release
November 2012

Human Dimensions in Cyber Operations Research and Development Priorities

Chris Forsythe
Cognitive Modeling

Austin Silva
Cognitive Modeling

Susan Stevens-Adams
Risk and Reliability Analysis

Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-1188

Jeffrey Bradshaw
Institute for Human and Machine Cognition

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.

These research and development investments would transform cyber operations from an art to a science, enabling systems solutions to be engineered to address a range of situations. Organizations would be able 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, the operational impact would be evident in improved performance, accompanied by a shift to a more proactive response in which defenders have the capacity to exert greater control over the cyber battlespace.

ACKNOWLEDGMENTS

The authors would like to thank and acknowledgement the following individuals who participated in the workshop and provided the valuable insights documented within this report: Myriam Abramson, Ben Apple, Susanne Bahr, Phillip Bennett, Ami Bolton, Ben Cook, Nancy Cooke, Jeremy Epstein, Kevin Farrell, George Jones, Ben Knott, Mike Lilienthal, Darren Lynch, Julie Marble, Ranjeev Mittu, Peter Muhlberger, Kevin Nauer, Chris North, Kelvin Oie, CDR James Patrey, Perry Pederson, Gabriel Radvansky, Stephen Russell, Ben Sims, Tom Starai, Ed Talbot, Rachel Wilson, Pam Savage-Knepshield and William Russell.

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.

CONTENTS

Acknowledgments 5
CONTENTS 6
List of Figures 7
List of Tables 8
NOMENCLATURE 9
1. Introduction 10
2. Workshop Participants 10
3. Structure of Workshop 12
3.1 Topic 1: What is the Problem? 12
3.2 Topic 2: How might the Problem be Addressed? 12
3.3 Topic 3: What can Cyber Leverage from other Domains? 12
3.4 Topic 4: What are the key Research Questions? 13
3.5 Topic 5: R&D Addressing the Human Dimension in Cyber Operations? 13
4. Topic 1: What is the Problem? 14
5. Topic 2: How might the problem be addressed 14
6. Topic 3: What can cyber leverage from other domains? 19
7. What are the Key Research Questions? 23
8. R&D addressing the human dimension in cyber operations? 25
8.1 What is the problem and why is it hard? 25
8.2 What are the limits of current practice? 26
8.3 What are the objectives and what difference will it make? 26
8.4 What are the measures of success/progress? 27
9.0 Conclusion 27
Appendix 1 28
Appendix 2 33

LIST OF FIGURES

Figure 1. The “Fulcrum of Power,” where the Defender is envisioned as the base of a fulcrum with the objective to flexibly move to one side or the other as needed to keep the user elevated. 15

Figure 2. This model emphasizes the feedback loops between operations (i.e. Cooke Model) and policy making, and the influence of users and adversaries on the overall system..... 16

Figure 3. Phases from development through procurement occur while not interfering with performance of current missions or associated assets..... 17

Figure 4. This model emphasizes two paths: one involving a rapid co-evolution that largely occurs at an operational level and a second slower evolution that involves a larger professional community. 18

LIST OF TABLES

Table 1. *Workshop Participants and their Organizational Affiliations*..... 11

Table 2. Opportunities and Lessons for Cyber from Analogous Domains..... 19

NOMENCLATURE

AWACS	Airborne Warning and Control Systems
R&D	Research and Development
S&T	Science and Technology

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.

There were four key objectives of the workshop:

- 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.

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. Experiences and insights were sought from across national security organizations with an underlying objective being the formation of a community of practice focused on science-based technological and organizational solutions to address the human element of cyber operations.

The workshop consisted of a series of focused discussions. The scope encompassed all areas impacting the effectiveness of cyber defenders in accomplishing their 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. The following sections correspond to the topics covered during the workshop and summarize the thinking expressed by the participants in the workshop.

2. WORKSHOP PARTICIPANTS

The workshop was coordinated and sponsored by Sandia National Laboratories and held at the Washington DC offices of the National Renewable Energy Laboratory. There were 32 participants representing 13 U.S. government organizations. Additionally, there were representatives from 6 academic institutions. In general, the backgrounds of participants

involved operational cyber defense, human factors and/or R&D program development and management. Table 1 provides a list of the participants and identifies their respective organizational affiliations.

Table 1. Workshop Participants and their Organizational Affiliations

Myriam Abramson	Naval Research Laboratory
Ben Apple	U.S. Navy
Susanne Bahr	Florida Institute of Technology
Phil Bennett	Sandia National Laboratories
Ami Bolton	Office of Naval Research
Jeff Bradshaw	Institute for Human-Machine Collaboration
Ben Cook	Sandia National Laboratories
Nancy Cooke	Arizona State University
Jeremy Epstein	National Science Foundation
Kevin Farrell	U.S. Navy
Chris Forsythe	Sandia National Laboratories
George Jones	CERT
Ben Knott	Air Force Research Laboratories (WPAFB)
Mike Lilienthal	Office Secretary of Defense
Darren Lynch	Lawrence Livermore National Laboratory
Julie Marble	Office of Naval Research
Peter Muhlberger	National Science Foundation
Kevin Nauer	Sandia National Laboratories
Chris North	Virginia Tech
Kelvin Oie	Army Research Laboratory
CDR James Patrey	U.S. Navy
Perry Pederson	Nuclear Regulatory Commission
Gabriel Radvansky	University of Notre Dame
Stephen Russell	Naval Research Laboratory
William Russell	Air Force Research Laboratories (WPAFB)
Pam Savage-Knepshield	Army Research Laboratory
Austin Silva	Sandia National Laboratories
Ben Sims	Los Alamos National Laboratory
Tom Starai	U.S. Navy
Susan Stevens-Adams	Sandia National Laboratories
Ed Talbot	University of California Davis
Rachel Wilson	Sandia National Laboratories

3. STRUCTURE OF WORKSHOP

The workshop consisted of five sections. In the initial section, participants introduced themselves and provided a brief personal perspective on the human dimension in cyber operations. At the conclusion of the workshop, participants were asked to provide a written one-paragraph personal perspective. These perspectives are provided in Appendix 1. Bios provided by workshop participants appear in Appendix 2.

Next, participants were divided into four work groups with each group assigned a leader. Participants were assigned to groups so as to assure each group was relatively diverse with respect to backgrounds and organizational affiliations.

For each of the remaining five sections of the workshop, teams were assigned a topic with specific objectives associated with the topic. These topics were chosen to engage groups in discussions that would progressively build toward a relatively complete consideration of the key issues and strategies for addressing the human dimension in cyber operations through science and technology research and development programs and policies. The topics and instructions provided to the groups were as follows:

3.1 Topic 1: What is the Problem?

Work groups were instructed to discuss how technologies, systems, organizations and cultures hinder the ability of cyber defenders to be fully effective and accomplish their mission. Work groups were cautioned that in their discussion, they should focus on general issues and avoid issues that are site or domain-specific, or technology-specific. The product of this section was a 60 second synopsis of the problem. In this synopsis, work groups were asked to imagine that they had 60 seconds to convince a key decision maker who did not appreciate the human dimension and was being encouraged to prioritize other research investments.

3.2 Topic 2: How might the Problem be Addressed?

Work groups were asked to assume that there is no single “magic bullet” for addressing the human dimension in cyber operations, but instead, the problem must be addressed through a multi-faceted, systems-level solution. The assignment requested that each group identify the elements of a systems-level approach to address the problem. Groups were asked to prepare a diagram identifying the elements and interdependencies between elements of their systems-level solution.

3.3 Topic 3: What can Cyber Leverage from other Domains?

The assignment asked groups to consider what problems involving the human dimension in other domains are analogous to problems posed by cyber operations. This assignment involved identifying instances of failures or accidents for which an analogous situation could occur in cyber and identifying success stories involving effective interventions that are relevant to cyber. Once this portion of the assignment had been completed, groups were asked to re-draw their

diagrams from the previous exercise to emphasize how elements in the diagram relate to both the failures and accidents, and success stories identified within other domains.

3.4 Topic 4: What are the key Research Questions?

Groups were instructed to again refer to their systems solution diagram and asked the question, "What do we need to know that we do not now know to implement the system solution?" It was requested that groups use a two-step process in which the first step involved their generating as many research questions as possible. Then, as the second step, they were asked to organize research questions into categories that reflected general topical areas. Once completed, they were asked to prepare a presentation discussing each topical area, and provide one or more examples of specific research questions for each topical area.

3.5 Topic 5: R&D Addressing the Human Dimension in Cyber Operations?

In the final section, groups were given two combined assignments. Having generated a categorized set of research questions, groups were first asked to prioritize these questions. The instructions called for a two-step process. In the first step, groups were asked to use the research topics they had identified and imagine that they had 10 funding tokens that they could distribute across research topics. The objective of this exercise was to elicit the groups' beliefs regarding the relative importance of topics. Once groups had completed the assignment of tokens, they were next asked to describe the strategy they had employed to make their decisions.

Once groups had prioritized the research questions, they were asked to prepare a proposal for a program of research and development to address these questions. Specifically, groups were given the following instructions, "Imagine you are one of several program managers competing to obtain funding for a new program of research and development." Groups were asked to first assume that there were sufficient funds for a large-scale, multi-year program to develop a comprehensive solution. Groups were also told to only address the technical elements of their prospective program and not to worry about funding, scheduling or other administrative matters. Finally, in presenting their prospective R&D programs, groups were asked to address the following four questions:

1. What is the problem and why is it 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?

4. TOPIC 1: WHAT IS THE PROBLEM?

The human is central to cyber security. At every step in developing and executing strategies to assure cyber security, humans are a vital part of both the process and the solution. The problem is present now and is mounting, and every day decisions are being made with the potential for regrettable consequences. Today, the cyber domain is the "Wild, Wild West," where anything goes and it is difficult to grasp the cumulative effects of deficiencies in technologies and practices. We may be on the verge of a "Cyber Pearl Harbor," in which the nation is shocked by a largely unexpected, extraordinarily impactful event for which we are ill-prepared to respond.

The technical, organizational and policy approaches currently being taken to address the human dimension of cyber operations are poorly calibrated to the problem, which is attributable to our not fully understanding the problem and the continually evolving nature of the problem. The threat is asymmetrical, both qualitatively and quantitatively, and places today's cyber defenders at an asymmetric disadvantage. Furthermore, unlike other threats, cyber does not adhere to the more readily grasped linear, continuous spatial-temporal models, which requires that the problem and solutions be conceptualized differently than other threats to national security that may be more easily defined.

Finally, cyber presents an interesting paradox. There may be no matter of national security where the public has a greater involvement. For example, personal home computers serve as hosts for many of the botnets that are the source of malware and phishing attacks. On the other hand, many current solutions place tremendous reliance on end-users taking prudent actions. Yet, the threat is evolving at a pace that is often too fast for policies, much less end-users, to adapt. Furthermore, a substantial (perhaps 80%) of the cyber infrastructure is owned and operated by public entities. Thus, any solution to address the human dimension in cyber operations must extend beyond government-controlled networks to address the public networks, and the public themselves, that may in various ways, touch the networks that we wish to defend.

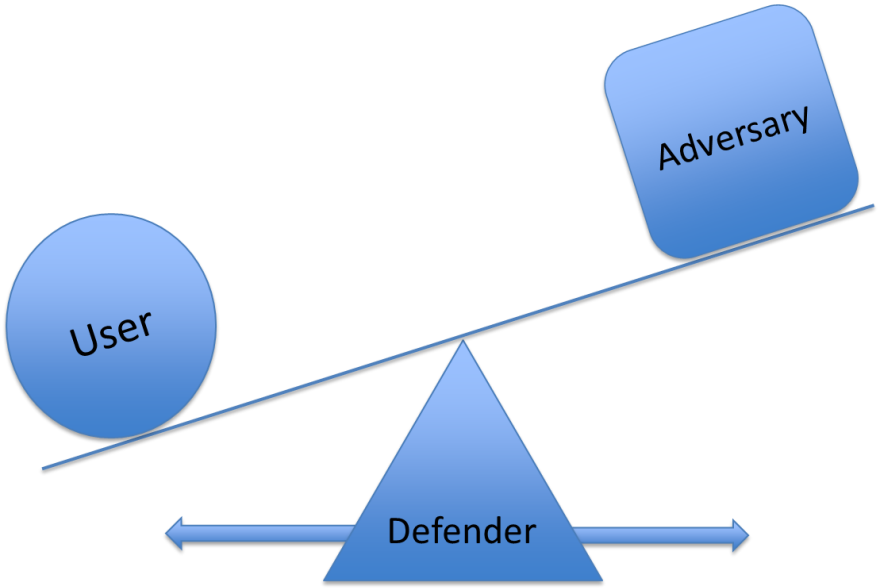
5. TOPIC 2: HOW MIGHT THE PROBLEM BE ADDRESSED

While there was considerable overlap in the ways in which groups conceptualized the problem, teams produced four distinct models in diagraming their prospective systems solutions. It should also be noted that for at least three of the teams, the chosen model was based on taking an existing model and elaborating and extending it to address cyber operations.

The first system solution, depicted in Figure 1, built upon the concept of a fulcrum. In this model, the problem is addressed by positioning the cyber defender at the base of the fulcrum. The defenders' role is to protect the system and the user while keeping the user "heavy" and maintaining its position in the center, and preferably on the ground. By being flexible in their defense, the defender can address the two groups in tandem but with various tactics and levels

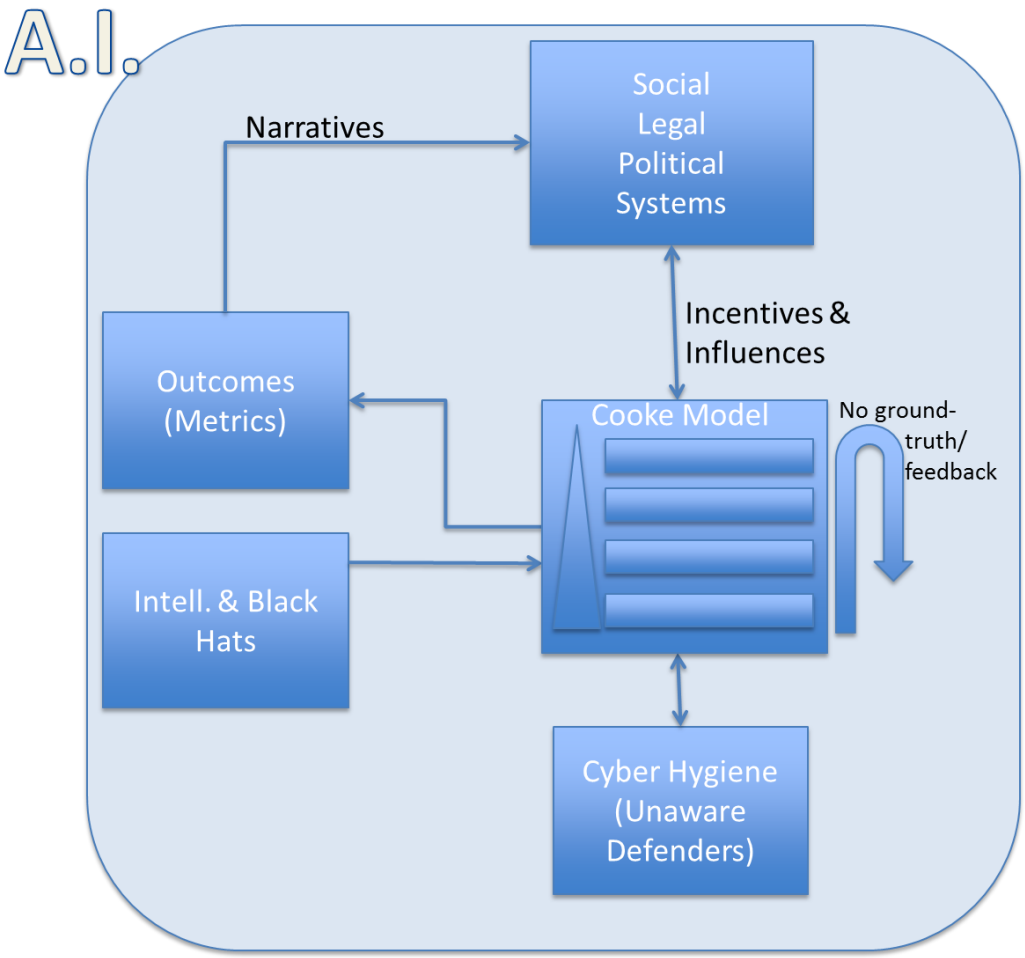
of attentiveness. It was noted that at times, the user may actually become the defender. This occurs when the user purposefully or inadvertently interacts with the adversary in some manner.

Figure 1. The "Fulcrum of Power," where the Defender is envisioned as the base of a fulcrum with the objective to flexibly move to one side or the other as needed to keep the user close to the ground.



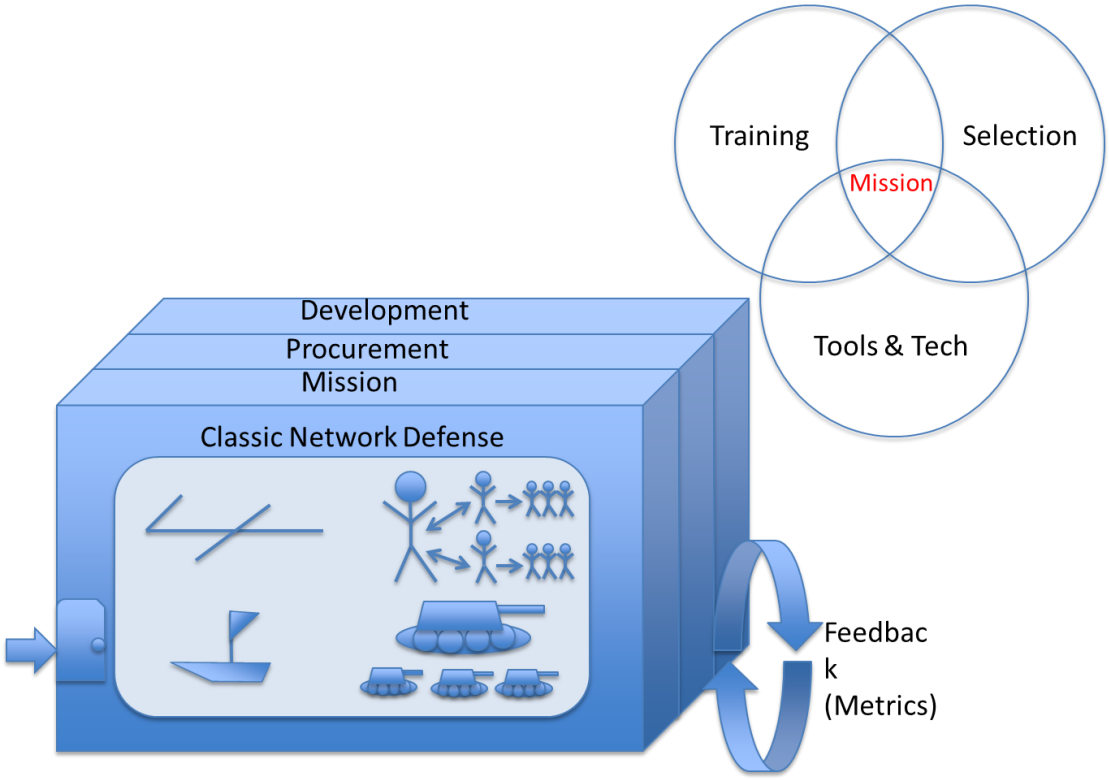
The second system solution, depicted in Figure 2, was built around a model of cyber operations that had been presented by Dr Nancy Cooke of Arizona State University during the initial perspectives briefings. Within the course of operations, outcomes and metrics are established that are turned into narratives that feed into the existing policy making structures (at the organizational level or beyond). These policies influence operations, yet activities at the operational level produce feedback that may influence the policy making process. Along the way, there are also external influences from adversarial entities and users that may impede the operational policies. Artificial intelligence and other technologies are included in this diagram to highlight the potential for automation to play various rolls in the overall system.

Figure 2. This model emphasizes the feedback loops between operations (i.e. Cooke Model) and policy making, and the influence of users and adversaries on the overall system.



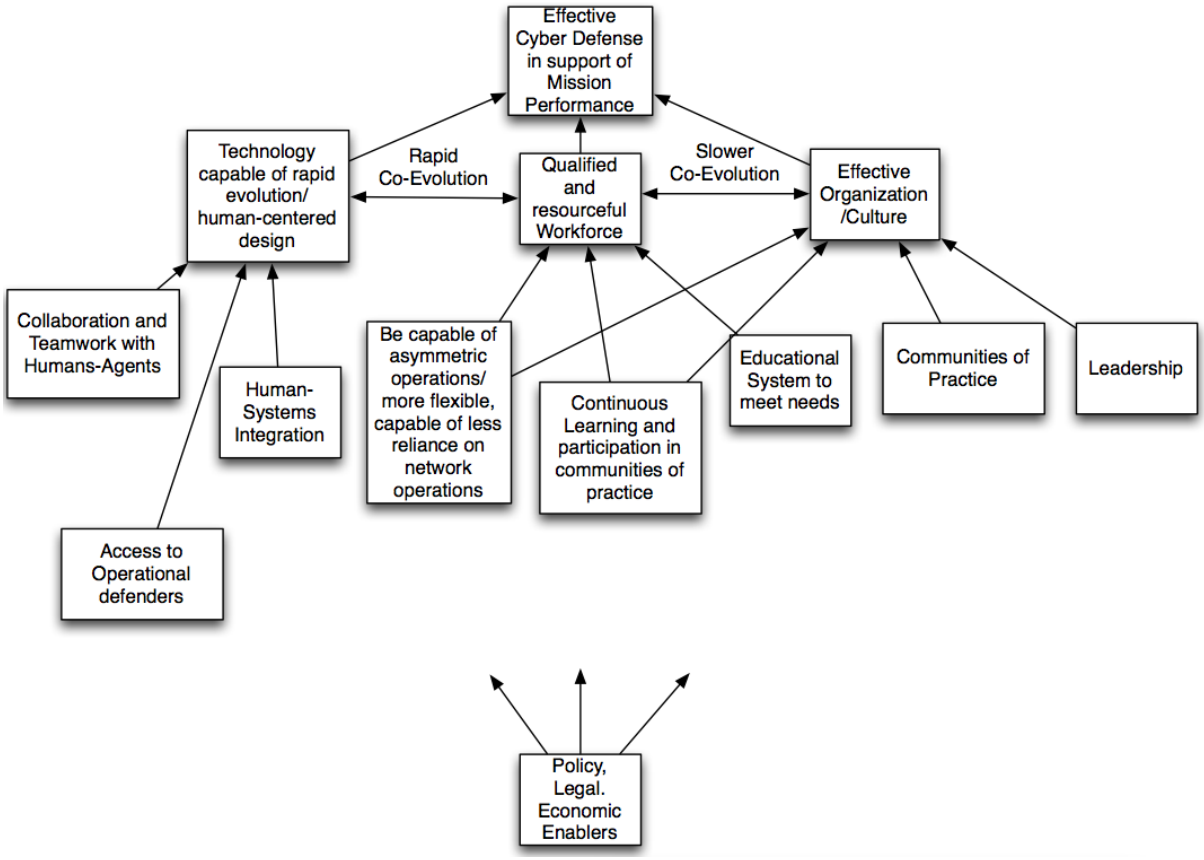
In the third system solution, the mission is the primary driver. Mission is best understood when the three following aspects are acknowledged: the training that is available and required, the process to select the best personnel and action, and finally, the technology and tools available. By understanding what the mission must support, solutions may emerge and supplementary procurement and development occur based on metrics and feedback that do not interfere with current operations or assets. This is depicted in Figure 3.

Figure 3. Phases from development through procurement occur while not interfering with performance of current missions or associated assets.



The centerpiece of the fourth solution, depicted in Figure 4, focuses on understanding the cyber defenders and developing a community that is grown to support their mission. There are two main tracks in this model: one that involves rapid co-evolution with the workforce and another that has a slower evolution. The fast-passed co-evolution involves technologies used by the defenders and harnesses human-systems integration, provides greater access to other defenders, and allows collaboration with human-agents. The slow evolution is supported by the leadership in the field as well as the development and trust of a community of practice. All fields, however, are affected by restrictions due to policy and economics.

Figure 4. This model emphasizes two paths: one involving a rapid co-evolution that largely occurs at an operational level and a second slower evolution that involves a larger professional community.



6. TOPIC 3: WHAT CAN CYBER LEVERAGE FROM OTHER DOMAINS?

Each team generated a set of analogies in which they identified other domains that exhibited problems similar to those attributed to the cyber domain. Based on these analogies, the following opportunities were identified for cyber to learn from the experiences of other domains. Table 2 provides a summary of the opportunities described in the following sections. These opportunities raise questions concerning the underlying factors, and the relative efficacy of alternative technical and organizational solutions.

Table 2. Opportunities and Lessons for Cyber from Analogous Domains

- Complex problems often require the integration of computer models and human judgment.
- Formalized, broadly institutionalized programs of education and training help to assure individuals are capable of responding to ambiguities.
- A culture may be instituted where reporting and sharing is the basis for a community of practice and continuous learning.
- Mechanisms are often needed to enable and promote collaboration between individuals possessing disparate pieces of a larger puzzle.
- Organizations and technologies may be structured to provide situation awareness and coordinated actions across distributed and loosely connected operators.
- Operators must be capable of coping with the attempts of adversaries to mislead and create a confusing tactical picture.
- Organizations and work processes must evolve at a pace commensurate with technologies.
- There is risk of mistaken and inadequate understanding of vulnerabilities.
- Effective personnel selection requires an understanding of what attributes are essential to an effective cyber defender.
- Cyber security requires the coordinated actions of a team, with there being a critical need for organizations, work processes and technologies to support teamwork.
- Opportunities exist to learn through reconstructive analysis of incidents involving cyber security.
- The human dimension in cyber operations may be becoming more supervisory in nature, and less a matter of experts applying heuristics.
- Learning and improvement require effective feedback mechanisms.
- The human dimension of cyber is a system-of-systems problem requiring an understanding of the many human-technology interdependencies.

Complex problems often require the integration of computer models and human judgment.
With weather forecasting, there is a similar need to assess massive amounts of complex data regarding current and historical trends. The objective is to anticipate events of moderate to severe consequences enabling appropriate preparatory actions to be taken, with there being the potential for extremely high consequence events. In this domain, data analysis and decision making processes have emerged that provide a reasonably effective integration of human judgment and the extensive use of computer models to aid in analyzing and interpreting data.

Formalized, broadly institutionalized programs of education and training help to assure individuals are capable of responding to ambiguities.
As in the field of medicine, cyber presents a nearly limitless opportunity for errors in human judgment and decision making. Likewise, medical practitioners must be on a constant vigil for clues indicative of unexpected developments prompting an immediate response. It is accepted that an effective practitioner must possess a rich mastery of a wide range of knowledge and demonstrate this mastery through a rigorous apprenticeship program. Furthermore, there are well-established standards that serve to assure the knowledge and capabilities of those allowed to practice at various levels and within different areas.

A culture may be instituted where reporting and sharing is the basis for a community of practice and continuous learning.
Commercial aviation was cited as a domain in which operators serve as a critical human-in-the-loop for a system that normally operates without incident. However, due to the need to function in dynamic environments and rely on complex technological systems, the human must be capable of effectively coping with critical situations that are relatively rare and may arise with little warning. In this domain, a community of practice has developed in which operators are expected to report their errors and lessons learned and rely on this sharing of information as a basis for their continuous learning.

Mechanisms are often needed to enable and promote collaboration between individuals possessing disparate pieces of a larger puzzle.
As with intelligence analysis, cyber operators must detect patterns corresponding to malicious activity, or intents, within vast quantities of data where the overwhelming majority of activity reflects the normal everyday pattern of life. Consequently, situations may arise in which all of the information needed to detect and comprehend adversary actions may exist in the hands of different operators without any of them knowing what the others know. Furthermore, where connections are made, these connections may rely on extraordinary efforts by individual operators, happenchance and the experience and personal connections of specific personnel.

Organizations and technologies may be structured to provide situation awareness and coordinated actions across distributed and loosely connected operators.
In the domain of wild land fire fighting, the threat (i.e. fire) may be broadly distributed across space and highly asynchronous with respect to when and where the threat might escalate. Consequently, in maintaining situation awareness, it is necessary that develop a broad

perspective that encompasses localized developments that may arise without warning (e.g. pockets of highly flammable materials), as well as larger scale developments with broad systematic effects (e.g. winds). Furthermore, this situation awareness must enable a coordinated response by individuals at distributed sites confronting the threat from different perspectives.

Operators must be capable of coping with the attempts of adversaries to mislead and create a confusing tactical picture.

With electromagnetic warfare, the objective is to maintain control of the electromagnetic spectrum and deny the enemy access to this spectrum. However, this occurs within a context where the adversary is constantly attempting to disguise their intents and lure the defender into committing resources to areas that are not actually being targeted. Furthermore, the defender may be forced to operate on the basis of an incomplete, and perhaps, inaccurate, knowledge of the adversary's capabilities. It was noted that a similar situation is also experienced with many games such as poker. With electromagnetic warfare, technological mechanisms, as well as training, are required that enable operators to develop and sustain an accurate tactical picture, as the enemy deliberately attempts to spoof and confuse the defender.

Organizations and work processes must evolve at a pace commensurate with technologies.

The experiences of the U.S. Air Force's AWACS platform was discussed as an illustration of the importance of an organization having the capacity to adapt with evolving technologies. In this case, significantly improved technologies were introduced to the aircraft; however, this technology was not compatible with the existing organization and work processes. This forced a re-organization of jobs and assignments to accommodate the new technologies. This example illustrates a situation where the technology outpaced the organization. This example is relevant in two ways. First, cyber defenders are the target of numerous groups developing various tools and technologies with the objective of improving cyber defense, but at the same time, potentially disrupting the work processes that enable organizations to sustain their network security. Secondly, the technologies interfacing with networks are continuously evolving, and as these technologies evolve, work processes evolve to take advantage of new capabilities, and efficiencies afforded by the new technologies. Consequently, the nature of the cyber defense problem and demands being placed on cyber defenders are evolving in concert with the introduction of these new technologies, often presenting new challenges for which there is limited opportunity for ample understanding of the threat or associated response.

There is risk of mistaken and inadequate understanding of vulnerabilities.

The fable of the Trojan Horse was discussed as an illustration of the potential for organizations to develop an erroneous mental model of their vulnerabilities and the imperviousness of their defenses. An analogy was made to the populous of Constantinople who believed their walls were so strong that the Greek attackers were incapable of defeating them. It was asserted that this misunderstanding is analogous to the reasoning that may be observed today with respect to firewalls, Link 16 and other mechanisms believed to afford a greater degree of security than

may actually be warranted. This observation points to vulnerabilities that lie within the assumptions and mental models that are prevalent within thinking regarding cyber defenses.

Effective personnel selection requires an understanding of what attributes are essential to an effective cyber defender.

Whereas in other occupations where there has been extensive investigation of the cognitive, psychological and physical factors that characterize superior performers, there is no comparable understanding of the factors that underlie an individual becoming an adept cyber defender. It was also noted that current practices frequently result in personnel lacking adequate qualifications being assigned to jobs as cyber defenders. Both fighter aircraft pilots and air traffic control operators were identified as occupations that faced a similar problem and have developed effective means for selecting job candidates with the highest potential to be successful.

Cyber security requires the coordinated actions of a team, with there being a critical need for organizations, work processes and technologies to support teamwork.

It was noted that with aviation mishaps, subsequent investigation has often revealed that a primary cause was the failure to pass information between different crew members. This has prompted development of crew resource management as a methodology for analyzing teams and developing work processes that assure effective information flow between team members performing different jobs. Similar analysis is recommended to understand the respective roles of members of cyber defense teams as a first step to understand information requirements of different jobs and develop more effective team processes.

Opportunities exist to learn through reconstructive analysis of incidents involving cyber security.

In other domains, it has become standard practice to employ various methodologies to assess and understand the chain of human reasoning that contributed to the occurrence of specific incidents. A common finding has been that these incidents do not have a single cause, but are the product of a number of contributing factors. Studies of this nature have the potential to provide insights into the thinking processes, assumptions and mental models, and their respective vulnerabilities that lead to breaches of cyber defense, with subsequent ramifications for work processes, training and the technologies being deployed.

The human dimension in cyber operations may be becoming more supervisory in nature, and less a matter of experts applying heuristics.

An analogy was drawn to chemistry where the early alchemist operated through a collection of heuristics passed down and improved from one generation to the next. Similarly, it was noted that more recently, a similar situation has occurred with finance. In the latter example, earlier traders had used rules of thumb and heuristics to interpret events and decide on appropriate courses of action. These heuristics have now been codified in software and much of the trading that happens today involves high-frequency, automated processes with there being a “war of algorithms.” Consequently, the role of the human has shifted from that of an active agent to that of a supervisor overseeing computers running various algorithms. It was asserted that as

more and more powerful tools and associated automation permeates the cyber security domain, the cyber operator is destined to experience a similar transformation from active agent to supervisor.

Learning and improvement require effective feedback mechanisms.
In the cyber domain, defenders must regularly operate not knowing ground truth. This was equated to the experience of remotely piloted vehicles where the operators have input from vehicle sensors, but during operations, they can only infer ground truth from the data available to them. In this domain, often, after the fact, ground truth becomes known and there exists the opportunity for feedback to be passed through the system based on this knowledge. This feedback provides the basis for learning and improvement for future operations. Within cyber, a similar opportunity exists where post-incident analysis may provide the mechanism for feedback to cyber defenders to allow their continuous improvement of operations.

The human dimension of cyber is a system-of-systems problem requiring an understanding of the many human-technology interdependencies.
An analogy was drawn to the commercial aviation system where there are numerous systems distributed across a vast complex network. Within such a system-of-systems, there is the potential for seemingly minor failures to have cascading effects throughout the system. Thus, human error at one point in the system can have severe ramifications at far-removed points within the system. It was asserted that the same situation exists with cyber operations where an otherwise innocuous human error at one point in the system can propagate through the system causing numerous seemingly unrelated failures at other points. This suggests the need for systems science approaches to understanding the human dimension in cyber operations and particularly, the potential for human-technology interdependencies, with this need being particularly pertinent given how difficult it can be to develop an accurate mental model of complex interdependent systems.

7. WHAT ARE THE KEY RESEARCH QUESTIONS?

Research questions fell into several somewhat overlapping categories. The following sections discuss the core issues underlying each of these categories.

Measurement and Metrics
Questions concerning measurement were fundamental to each of the categories of research and represent an area in which there is a need for foundational research. 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. A desire was expressed for a testbed capability engineered to enable fundamental

questions to be answered regarding the cognitive science underlying the performance of cyber defenders, teamwork, communication, technologies and alternative modes of training. Furthermore, there is need for measures that may be implemented within operational settings as a basis for ongoing assessment and feedback for continuous improvement. However, once measurement moves from the laboratory where ground truth may be known to operational settings, issues arise concerning how to conduct measurement in settings where it is not possible to know ground truth with absolute certainty.

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. This basic understanding is seen as a preliminary step to research addressing other key questions such as the existence of cognitive biases, role of communications, use of narratives and susceptibility to the influence and diversions of adversaries.

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. Of particular importance, questions exist concerning how knowledge of adversaries, including models of adversaries, may be effectively operationalized. Ideally, cyber defenders would have a range of tactics and techniques, and potentially, supporting technologies, available to them providing various measures to influence the beliefs, motives and behaviors of adversaries.

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. It was emphasized that training extends beyond the training environment and that research was needed to explore the use of operational data as a basis for feedback in continuous improvement. Finally, training may occur at multiple levels covering a range beginning with the individual and extending outward to encompass teams, groups, the organization and multiple organizations, and it is unclear what the right mix and amount of training for each level might be.

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. There are broad ramifications of knowledge concerning what makes for effective team operations in the cyber domain, with this knowledge having impacts upon operations, technologies, training, and organizational structures and processes. Extending beyond the interactions that occur within teams and organizations, there is also need for research to explore methods to enable and promote productive collaboration across organizations.

Understanding the User

While the objective for the current analysis has been to identify R&D priorities related to cyber defenders, there was considerable discussion of end-users, with the proposition that at some level, every end-user is a cyber defender. Furthermore, operational cyber defenders stand to benefit from a better understanding and ability to anticipate and influence the behavior of end-users. Key questions concern what characteristics and conditions make end-users more or less vulnerable? How do you measure the effectiveness of end-users as cyber defenders, as well as the impact of policies and other actions on affecting the behavior of end-users? Finally, what factors influence end-user perceptions of the threat and what measures may be taken to alter their beliefs and actions?

8. R&D ADDRESSING THE HUMAN DIMENSION IN CYBER OPERATIONS?

Each group developed a distinct, yet somewhat overlapping research proposal. In reporting the outcome of this exercise, 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.

8.1 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.

8.2 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.

8.3 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.

8.4 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.

9.0 CONCLUSION

The preceding sections outline a proposal for a program of R&D to address the human dimension in cyber operations. The objective of this 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.

APPENDIX 1

Workshop participants were requested to present a brief personal perspective concerning the human dimension in cyber operations during the initial session of the workshop. At the conclusion of the workshop, participants were asked to re-assess their perspective based on the discussions that occurred during the workshop and prepare a written perspective. The following written perspectives were submitted by the workshop participants.

Myriam Abramson, Naval Research Laboratory

My perspective coming up into the workshop, given my background and my current research, is that cyber defenders need sensemaking tools to understand behavior on the network. My current research is concerned with the attribution of Web browsing behavior which could be useful to detect masquaraders and unusual behavior by constructing user profiles. Cyber attacks occur too fast for human decision making to take place so a lot of emphasis has to be placed on automated cyber defense, for example, automatically shutting down nodes that have been compromised on the network, validating users based on inferred cognitive fingerprints rather than passwords, etc.

So, where is the human dimension in cyber defense? The human seems to be the weakest point in cyber security. What I got from the workshop was that, whether we like it or not, the human is everywhere. Automated cyber defense need to be accepted from a socio-cognitive perspective if nothing else. For example, privacy issues might prevent surveillance of the network for protection purposes. "All warfare is based on deception" is even more true in cyberwarfare. How to train people against deception? Moreover, deception in cyberspace is everchanging. For example, a good link one day could become infected the next day. The enemy is hidden and amorphous. Cyber defense might become a way of life just like our immune system protects us from diseases and this metaphor has been used to construct adaptive cyber security systems. But are we ready for it? I know for one that I cherish the control that my command line capability on Linux gives me.

What cognitive and social scientists can do is to enable our acceptance of this intelligent cyberspace/battlespace environment through training and promotion of norms and incentives. There is a lot of interest in enabling autonomy at ONR mainly because of the increased use of UAVs and robots on the battlefield. I think a larger perspective needs to be taken to include autonomy in cyberspace as well.

Beyond the analysis of the problem, the possible solutions coming out of the workshop seemed to only scratch the surface of the problem. Maybe groupthink settled in the second day :-)

Jeff Bradshaw, Institute for Human and Machine Cognition

Despite the significant attention being given the critical problems of cyber operations, the ability to keep up with the increasing volume and sophistication of network attacks is seriously lagging. Throwing more computing horsepower at fundamentally-limited visualization and analytic approaches will not get us anywhere. Instead, we need to seriously rethink the way

cyber operations tools and approaches have been conceived, developed, and deployed. Though continuing research to improve technology is essential, the point of increasing such proficiencies is not merely to make automated tools more capable in and of themselves, but also to make analysts more capable through the use of such technologies. To achieve this objective, we must adopt a human-centered approach to technology development. Unlike current approaches, human-centered design requires a co-evolution of the user task and the technology artifact, as expressed two decades ago in Carroll's task-artifact cycle. The task-artifact cycle includes two phases: the first involves the design and development of artifacts to help users perform their assigned tasks; the second concerns the way that the use of the artifacts defines new perceptions, possibilities, or constraints of use that change the way the task is performed. Though the concept is a good one, the development cycle as typically implemented is too slow to keep up with the fast pace of change in threats and analyst practice. To speed up the process of parallel evolution of tasks and work practices, we have proposed tools and methodology based on the concept of coactive emergence, an iterative process whereby joint sensemaking and decision-making activities are undertaken in tandem by analysts and software agents.

Nancy Cooke, Arizona State University

Prior to the workshop my perspective on cyber operations was based on my experience working on the USAF Scientific Advisory Board study on cyber situation awareness as well as on an Army Research Office Multidisciplinary University Research Initiative (ARO MURI) on cyber situation awareness. Based on this experience and cognitive task analyses done for the ARO MURI, I have come to see cyber defense as a sociotechnical system with multiple humans and machines participating in a layered set of tasks, starting with cyber triage done by analysts, moving through escalation analysis, correlation and threat analysis, and finally mission assurance for the commander. Each of these cyber tasks requires distinct cognitive processes such as monitoring, sensing, inspecting, synthesis, and decision making and each process can be allocated to human, machine, or some combination of both. Challenges to the sociotechnical system that are limitations for it today include inadequate allocation of cognitive task to humans and machines, as well as limited coordination and communication through the system especially from the top down to help guide analyst expectations.

Since the workshop I have come to appreciate that the sociotechnical system is actually broader in scope. In fact, I have become convinced that cyber hygiene of the public is a central problem and that the public as the first (but mostly unwitting) line of defense, needs to be included in this system. The military bemoans the problem of poor cyber hygiene on the part of the public, but I think the problem is that the public is unaware of their role in cyber operations and is therefore not motivated to practice reasonable cyber hygiene. What is needed is a public awareness program to inform the public about their roles and the ramifications of poor cyber hygiene. In addition to the importance of the public's role, my belief that quality research in this area will depend on viable testbeds and metrics was reinforced in this meeting.

Chris Forsythe, Sandia National Laboratories

In an interview for Wired Magazine, Steve Jobs discussed his philosophy for design. He asserted that there are three stages. In the first stage, there is not an adequate understanding of the problem or the constraints, and as the result, designs tend to be overly simplistic. In the second stage, based on the lessons learned from the first stage, there is an effort to address the various problems and in doing so, complexity is added to the design. Initially, this increased complexity produces a better design, however there is a point of diminishing returns and the improvements that come with further increases in complexity become less and less. Eventually, a ceiling is reached where no further improvement can be attained with additional complexity, yet the product remains unsatisfactory. The final stage comes when the "essence' of the problem is understood and the solution, which is generally relatively simple becomes obvious. It is arguable whether today cyber is in the first or second stage of this process, and cyber is certainly nowhere close to the third stage. Furthermore, cyber runs the risk that the domain may become stuck in the second stage with the allure that effective solutions can be had with just enough engineering and added technical complexity. What cyber needs are efforts that push toward an understanding of the essence of the problem and allow cyber to shorten the period spent in stage two and progress toward the simple, yet elegant solutions that arise from stage three.

Chris North, Virginia Tech University

Cyberspace is still in its early "wild west" days. There are few standards and rules, little enforcement infrastructure, and each citizen is his own defense. Advancing to civilized society in cyberspace requires progress in numerous research fronts. One such front is to enable the professional cyber defender. In this arena, the strategic nature of cyber defense requires human intuition, but the massive scale of complete connectivity requires automation. However, cyber defenders are wary of new visualization and algorithmic tools that are developed in research environments with the intent of supporting cyber defense activities, because these tools typically give them yet more mined information to attend to or hide important information behind overly aggregated dashboards. Research is needed to progress beyond current "human-in-the-loop" paradigms where human and machine occasionally meet to compare results, to a "human-IS-the-loop" paradigm where algorithms fit seamlessly into human sensemaking processes; where algorithms continuously learn from and respond to human intuition during the course of the cyber defenders ongoing analysis. For example, algorithmic parameters and outputs must be re-cast to fit naturally into defenders mental models and interactive processes. New approaches to interaction, such as large-scale visual spaces, are needed to enable cyber defenders to effectively manipulate large-scale automation. Accordingly, a well-enabled professional cyber defense will transform chaos to order.

CDR James Patrey, U.S. Navy

The key challenges of the cyber domain are intertwined with those of the physical world of our operational domains, such as the Naval aviation domain. One of the fundamental concerns in this domain is the complexity and volume of information being presented to our individual pilots and aircrew in both our manned and unmanned cockpits. The ability to connect airborne craft with the cyber domain creates incredible opportunities along with dangers as we discern

how to enable the cyber domain to enhance aviation performance and avoid information overload. This becomes especially critical as we incorporate net-enabled weapons with our manned/unmanned aircraft and embark on rapid and informative data exploitation from our Intelligence, Surveillance, and Reconnaissance (ISR) platforms and sensors. The warfighting domains rely on the cyber operators to preserve the integrity of our cyber domain and the incoming/outgoing communications (along with disrupting those of our adversary) , but organic shipboard assets must also aid in this preservation as a second-line cyber operator through direct monitoring and management of shipboard/airborne systems and our aircrew must learn to be an effective third-line cyber operator as both a wise consumer of information who can identify and defend against spoofing, jamming, and other assorted cyber attacks along with perpetrating such electronic warfare attacks in theater. The tools and techniques to accomplish such effects, along with clarity on the skills and training needed to implement them, are at best incomplete and often do not exist, posing a significant constraint in our cyber operations, one which should be met with a concerted effort to understand how to best implement the human in the cyber domain.

Gabriel Radvansky, University of Notre Dame

My main interests are in memory, comprehension, and narratives. One of the issues in cyber-security is understanding the narratives people create for themselves of their own role in the triad of the user, the cyber defender and the attacker. By understanding the causal and enabling structures in such narratives, it becomes possible to understand how these can both facilitate and hinder performance, particularly of the cyber defenders. This approach also can serve as the basis for understanding some of the beliefs, motivations, and actions of users, defenders and attackers. In terms of the user, this can help provide a better understanding of why they sometimes leave themselves open to attack, and how to modify their narratives to promote a more self-protective posture. In terms of the cyber-defenders, this can provide a better understanding of how they interact with both users and attackers, and how to better direct their attention away from non-compliant users, and aim their efforts more at the causal source of the problem, the cyber-attackers. Finally, in terms of the attackers, this can provide a better understanding of how they view themselves and others and provide the foundation for taking steps to break or alter their self-narratives. The aim of such activity would be to deter such people from engaging in cyber-attacks, or to limit the kind of attacks that an attacker is motivated to try.

Benjamin Sims, Los Alamos National Laboratory

The field of operational cyber security is at a critical point on the path toward professionalization. What had been an aspect of the work of system and network administrators is increasingly handled by specialized practitioners, who have been coming together as a community to develop their own work culture, practices and standards. However, as with any nascent profession, there are many issues that have not yet been resolved, such as: What kind of education and training are appropriate for cyber security operations work? How do practitioners move from being novices to being expert in the field? Are there specific cognitive and personality traits that contribute to job performance? Are there barriers that steer people away from cyber security who could be effective experts? What sub-specialties

exist in cyber security work, and do these require specialized training or experience? Do cyber security operations personnel work effectively as teams, and what contributes to team effectiveness? Are cyber security tools and technologies effectively supporting the cognitive demands of the work environment? How can we measure the effectiveness of cyber security operations personnel and teams? Answering these questions will require significant investment and collaboration between cyber security experts and social and behavioral scientists from fields like sociology, anthropology, cognitive science, and psychology.

It is useful to consider three dimensions of professionalization in relation to cyber security operations: professional structure, professional practice, and pathways to membership in the profession.

Professional structure typically involves establishing a community of practitioners, mainly through professional meetings and conferences, developing standards and requirements for membership in the profession, and gaining control over a particular domain of practice to the exclusion of other professions. Cyber security has some of these features, such as meetings and conferences, and a number of professional organizations exist, but the field has few formalized standards for professional membership, and lacks a unified professional structure.
Professional practice is related to the key problems and tasks in a field, the tools, technologies, and mental and cognitive models used by practitioners, and division of labor and team dynamics in the workplace. The field of cyber security has some amazingly skilled practitioners, but there has been little work done to establish best practices for how these individuals should work as teams within organizations.

Finally, professions need to establish pathways to membership that filter out poor candidates and draw in a wide range of the best possible candidates. This typically involves developing standards for effective education and training programs, understanding and mitigating barriers to entry into the field by qualified candidates, providing mentorship and growth opportunities for new professionals, developing a pool of highly expert practitioners, and creating a dedicated cadre of professional leaders. While there are a number of effective training programs and opportunities in the field of cyber security operations, more effort is needed to understand what kind of educational and work experiences create effective practitioners and leaders, and to understand what draws people in or steers people away from the field so that a steady stream of competent new practitioners can be established. Social and behavioral science research can provide valuable insights into how to address these issues.

APPENDIX 2

Workshop participants provided the following brief bios.

Myriam Abramson, Naval Research Laboratory
Myriam Abramson is a computer scientist at the Naval Research Laboratory. She obtained her PhD in computer science for algorithms coupling neural networks with reinforcement learning at George Mason University in 2003. She is currently conducting research in Web behavioral analytics.

Jeff Bradshaw, Institute for Human and Machine Cognition
Jeffrey M. Bradshaw (Ph.D., Cognitive Science, University of Washington) is a Senior Research Scientist at the Florida Institute for Human and Machine Cognition (IHMC) where he leads the research group developing the KAoS policy and domain services framework for network management and the coordination of human-agent-robot teamwork. With Marco Carvalho, he co-leads the development of the Luna Software Agent Framework and the Sol Cyber Framework. Selected Publications on these and other research projects are online at www.ihmc.us/groups/jbradshaw/

Nancy Cooke, Arizona State University
Nancy J. Cooke, PhD is a professor of Cognitive Science and Engineering at Arizona State University. She is also Science Director of the Cognitive Engineering Research Institute. Dr. Cooke's research focuses on human systems integration and in particular, team cognition and metrics for assessing team cognition.

Jeremy Epstein, National Science Foundation
Jeremy Epstein is the lead Program Director for the National Science Foundation Secure and Trustworthy Cyberspace (NSF SaTC) program, which is NSF's primary cybersecurity research program. Jeremy is on loan to NSF from SRI International, where he focuses on software assurance and voting system security.

Chris Forsythe, Sandia National Laboratories
Chris Forsythe is a Distinguished Member of Technical Staff in cognitive science and technology at Sandia National Laboratories. He has led a variety of efforts focused on the application of technology to improve human performance across various domains. A particular emphasis has been the use of instrumentation as a mechanism for capturing data regarding human performance for continuous performance improvement within both training and operational contexts.

Darren Lynch, Lawrence Livermore National Laboratory
I started in desktop support 15 years ago and worked my way up to server support and infrastructure support for the Active Directory environment; in the process I was able to learn the technical depth and breadth of knowledge of physical networks and hardware. I have been

part of computer security since May of 2012 at LLNL with a customer and clientele focus for building relationships to better enhance the progress of computer security throughout the industry.

Chris North, Virginia Tech University
Dr. Chris North is an Associate Professor of Computer Science at Virginia Tech, where he leads the Information Visualization research group in the Center for Human-Computer Interaction, and directs the GigaPixel Display Laboratory. His recent research interests focus on visual analytics, user interfaces for large high-resolution display spaces, combining interactive visualization with computational data mining, and insight-based evaluation methods for visualization. He earned his Ph.D. at the University of Maryland, College Park, in 2000.

CDR James Patrey, U.S. Navy
CDR Jim Patrey is a U.S. Naval Officer and an Aerospace Experimental Psychologist in the Navy's Medical Service Corps, commissioned as an officer in the US Navy in 1997 and attended Naval flight school in Pensacola, FL after earning a Ph.D. in Cognitive Psychology at the University of Illinois. He has served in diverse assignments at the Naval Air Warfare Center Training Systems Division, United States Air Force Academy, Office for the Assessment and Review of Detained Enemy Combatants, Aviation Training Systems Program Office, and the Office of Naval Research. CDR Patrey is currently the Assistant Director of Science and Technology in the Human Systems Department at the Naval Air Warfare Center Aircraft Division.

Gabriel Radvansky, University of Notre Dame
Gabriel Radvansky has been a professor at the University of Notre Dame since 1993. His research focuses on memory, comprehension, narratives, and aging.

Benjamin Sims, Los Alamos National Laboratory
Benjamin Sims holds a PhD in Sociology and Science Studies from the University of California, San Diego. He is currently a scientist at Los Alamos National Laboratory, where his work addresses weapons safety, infrastructure reliability, and cyber systems and security. His research interests include scientific and professional work and organizations, risk and safety in socio-technical systems, and social aspects of breakdown, repair and retrofit.

Tom Starai, U.S. Navy
I am the chief engineer at the Navy Cyber Warfare Development Group which is the R&D component of Fleet Cyber command. My interest in the workshop subject is to add cognitive models to constructive simulations for assessments, planning and optimization. I am looking to share and collaborate and appreciate the community of interest reflected in the workshop.

Distribution

1	Phil Bennet, 1463		
1	Benjamin Cook, 5624		
1	James (Chris) Forsythe, 1462		
1	William Hart, 1464		
1	Kevin Nauer, 9312		
1	Austin Silva, 1462		
1	Susan Stevens-Adams, 6231		
1	Technical Library, 9536 (electronic copy)		
1	MS0359	D. Chavez, LDRD Office	1911


Sandia National Laboratories