The Cognitive Sciences of Cyber-Security: A Framework for Advancing Socio-Cyber Systems

Michael D. McNeese(✉) and David L. Hall

The Pennsylvania State University, University Park, PA, USA
mmcneese@ist.psu.edu

Abstract. Traditionally, cyber security has been positioned and developed primarily from a computational-technology perspective. Unfortunately, this has been rather short-sighted as it provided solutions that fail to consider many human-related, cognitive, and social factors that underlie solutions of significance. While there have been substantial contributions from technology development that help the overall problem, a more comprehensive and effective approach is now needed that: (a) explores cognitive sciences and collaborative systems as a substantial basis to reify discovery and prediction, (b) produces incisive research results that inform the design of cyber tools and interfaces for active use, and (c) establishes new understanding of cyber situation awareness wherein the distributed cognitive activities of users, dynamic and changing roles of the threat and the environment, collaborative teamwork, and the promise of innovative cognitive technologies are intertwined and realized. This chapter outlines the perspective of social-cyber systems, a transdisciplinary approach designed to enhance information protection, reduce errors and uncertainty, take advantage of teamwork, and facilitate insightful understanding of what awareness and collective induction means for cyber defense and security. The Living Laboratory Framework is used to describe our approach and to implement specific aspects of social-cyber system research that inform dimensions of awareness and induction. Cognitive explorations underlying cyber situation awareness are presented that involve entwining theoretical foundations, models and simulation, and problem formulation - with - ethnographies of practice, knowledge elicitation, design storyboarding and technology prototyping. Integration of these important elements provides the basis of expanding individual cognitive processing into collaborative teamwork and collective induction that afford the goals of obtaining readiness and resilience in social-cyber systems. Finally, the chapter looks towards what future requirements will be necessary to sustain efficacy in protecting valuable resources and services.

1 Background

Cyber security can mean many things to many people but it is clearly one of the most daunting problems that impacts society today. Not only is it a problem associated with the military or intelligence assets of the United States and other countries, the security of our existence as human beings may be at stake if catastrophic consequences of poor

P. Liu et al. (Eds.): Cyber Sitation Awareness, LNCS 10030, pp. 173–202, 2017.
DOI: 10.1007/978-3-319-61152-5_7

cyber security ensue. Cyber security threatens our lives and our lifestyles with ubiquity unparalleled. It may open up our bank accounts for massive loss, threaten the loss and theft of identities, the security of the transportation systems we use, decimate our energy infrastructure, and can make our defenses that thwart nuclear attack nil. Indeed, cyber security breakdowns are one of the most-wicked problems (Churchman 1967) that besiege humanity in the present days.

In today's world cyber security events and situations unfortunately occur on a regular basis, with some having more serious consequences than others. Since the beginning of 2015 major cyber security events have happened. The most recently leaked data on "Ashley Madison" accounts provides a significant example of how cyber security hacking and data access can reach deep into the societal backbone. Ashley Madison represents an online dating site, which essentially facilitates extramarital affairs for adults who are currently married. In July of 2015 the site was hacked by a group called "The Impact Team" wherein the database of 31 million customers was exposed. This made personal information highly vulnerable and has opened-up other problems. One problem is that the database contained 10,000 customers who were government / military workers. It is surmised that this has compromised national security concerns along the lines of extortion-blackmail, placed sensitive projects at risk, and help adversaries further target cyber security attacks on intelligence data [see <http://thehill.com/policy/cybersecurity/251517-cyber-foes-likely-digging-through-ashley-madison-data>]. Because this event just happened, the spreading activation effects are not yet fully known. But this example demonstrates that hacking is not just a one-time hack that exists at the surface but really creates a complex, emerging situation that has multiple, deep layers. The perception of what cyber security is can be very rigidly defined around the computers, architecture, and data but the perspective that is necessary is more expansive, and needs to consider "awareness" around the broader notions of people, behavior, crime, and society in order to develop compelling solutions. Awareness in cyber security is not simply developing new technologies or computational algorithms but must consider the cognitive sciences that underlie intelligence, behavior, and action.

At the heart of cyber security philosophy, policy, and operations is the adversarial imperative, which imparts a threat to take ownership of computer infrastructure, system, and/or files that maintain data, information, and knowledge that is often critical for preservation. Because computational intelligence is distributed in many ways (smart phones, reservation systems, navigation, cameras, military systems and so on) it makes the cyber threat even more serious and potentially devastating. Cyber security operations are targeted upon technology but they are initiated by human intelligence – designed to control or take over human enterprise, social and political entities, and to destroy what we value as humans. In turn cyber security is concocted by humans against humans and is designed to obtain the 'upper hand' of either control, execution, power, or dominance. Because it is foisted against us – strong programs of immunity from its effects must be initiated and sustained with much creativity and innovation. What makes this so difficult is the lightning quick 'change of state' in which cyber security effects can initialize and dissipate. Couple this much a maximum amount of duping, deception, and disruption and one is facing one of the most-wicked problems possible.

This chapter is derived from our joint effort at Pennsylvania State University (along with a team of other universities) to understand what cyber security means from the perspective of situation awareness. For several years we have been engaged in a Multidisciplinary University Research Initiative (MURI) designed in increase our knowledge about situation awareness within cyber security. This is a grant provided by the Army Research Organization (ARO) and represents a broad bandwidth approach to thwarting threat operations that are predicating on awareness (or lack thereof).

As a point of full disclosure the position that presented in this chapter is one that focuses around the worldview of cognitive science and necessarily is human-centered in view and application. Cyber security is considered from the intersections of information, technology, people, and context to derive knowledge about dynamic awareness and how it emerges over time. While we value the worth and usefulness of technology, we have seen within circles of the human factors that technology is often developed without consideration of human, social, or contextual factors that strongly imprint on its use. This chapter is not anti-technology but instead, uses an interdisciplinary nexus to develop technology that achieves situation awareness where the human is informed and can act in their environment in a way that produces tactical or strategic advantage in the course of achieving an objective. The hope behind this chapter is to introduce some alternative ways of interpreting awareness within cyber security, wherein new innovative thinking and creative design can make a difference in our lives.

2 Introduction

It is no surprise that we conceptualize cyber security as an interdisciplinary system of systems where transformative work is both local and distributed but undertaken by human agents engaged with other agents (human or computational) within an often changing environmental context. From this view, cyber security is human centered and requires human-in-the-loop processing, contextually driven by change, and must be approached and addressed through problem-based learning. As part of our MURI progress (over the last 6 years) – we have held on to the basic idea that if an analyst or team of analysts can obtain and maintain situation awareness during the course of problem solving, they will be successful in protecting systems and enhancing cyber defense readiness. The timely integration of information, technologies, people, and context are all important for considering cyber security as an interdisciplinary system of systems, team of teams conceptualization Cyber security is a very challenging problem space that contains multiple layers of complexity that can emerge and evolve quickly in many different ways. Activities within cyber security problem space can be seen as dis-granular and nonlinear as well as it contains virtual non-physical space (e.g., where hackers attack a software-based system designed to protect computer security), as well as physical cyber security elements, often, which are bridged together through human cognition and action. When considered jointly these elements create a demanding context for establishing situation awareness, and produce what has been referred to as wicked problems (Churchman 1967).

Conceptualizing Cyber Security as Distributed Cognition

For the purposes of this chapter it is necessary to begin with what we consider cyber security to be (i.e., a basic definition that characterizes it as a specific area of focus that is real and exists within a situated context). Therein, we will begin with the following definition (McNeese et al. 2011):

> By cyber security we mean a socio-technical system of a vast array of distributed computers, servers, and analysts designed to protect users from: (a) compromised systems and vulnerabilities perpetrated by adversarial threats and (b) defined and acted upon by humans for humans using computer-based tools.

While this definition is straightforward and specific and describes what cyber security 'is' - it is now four years old and may be too static of a definition. To update this definition, we now believe that cyber distributed cognition occurs in what we might term cyber-worlds – a virtual interactive world that can be veiled, hidden, and often deceptive; that consists of multiple, dynamic layers that can change dimensionally, representationally, numerically, and in many other ways within milliseconds (i.e., lightning quick). Cyber worlds contain socio-cyber systems that consist of a series of human-environment transactions wherein a team of teams utilize many tools and infrastructure inclusive of intelligent computational agents acting as teammates, web-based sensor data fusion, the internet of things, cyber visual analytics, and social network prediction. Socio-cyber systems are exactly the contexts that cyber analysts work within to address, manage, and attack where the adversary seeks to gain entrance to destroy data, exploit information, and/or take control.

Traditional notions or models of cognition get stretched and changed in cyber-worlds as there are unique information-context interdependencies that emerge and change rapidly in time and space within the social and physical environment. Space in this context is different from typical physical context wherein physics play out laws of nature. Space in cyber worlds is bound within the constraints of "what is possible" given the software boundaries, the disguise that data may take on, and the lightning speed of rapidly changing states within this unique kind of conceptual space. This is different than tracking a physical threat of the battlefield wherein movements of targets are subject to D = R*T physics and other constraints. Change of this magnitude means cognition and awareness addressing the current state of cyber operations is more difficult to comprehend, and perhaps learn. Information half-life (recency) becomes incredibly hard to decipher especially in non-routine situations. This is the world we expect a human to understand and comprehend to thwart cyber threats as they manifest in different kinds of modalities and environments (e.g., smart phones, banking systems). As indicated with the above definition cyber worlds must include human interpretation and that interpretation is assisted by technologies that bring forth new tools, interfaces, and simulations that enhance our ability to be active responders, to 'see' differently, and to predict patterns before they come to fruition. The demands placed on cognition are not just analytical but include the ability to induct, to learn deep elements of patterns that form in cyber worlds, to create and intuit, and to discern when deception is in process.

Worldviews of Cognitive Understanding. The world of cyber security takes place within a complex environment (as they denoted above as a cyber-world) that may be conceptualized from a number of different worldviews (mathematical, computational and information science, business intelligence, eco-systems, criminological-terrorist studies, social informatics, information fusion, big data analytics, cognitive-psychological science, to name a few). Historically, situation awareness (Endsley 1995) has primarily been addressed from a cognitivist worldview where an analyst utilizes "cognition as being in his/her head" and then applies it as apropos. This view is predicated on older human information processing approaches to cognition (Newell and Simon 1972) where cognitive understanding is equitable or analogous to a computer elements reading data into a central processing unit (e.g. image translation, memory storage) then appropriating responses via output mechanisms). Cognivistic models have been around approaching 60 years (Newell et al. 1958) and perhaps much longer if one considers philosophic predecessors (e.g. Descartes 1664). The cognitivist view has been challenged as too microscopic (micro-cognition is often too static and relies on a homunculus in the head (but who directs this master controller?); micro-cognition under-estimates the impact of the environment or context that affords action, and often micro-cognition fails to consider the social/teamwork aspects of cognition in terms of emergent dynamics.

In turn, another perspective has emerged which may be termed an ecological-contextualistic worldview. Historically, this view has evolved from the early work of James Gibson (1979) based on his research in direct perception which in turn focused on human-environment transactions, and the role of affordances and effectivities have in specifying information. Action and perception of are jointly determined by an actor within a context (Greeno 1994). A contextualistic approach (Hoffman and Nead 1983) looks at cognition as also being distributed outside the head in the environment. A human often constructs or picks up information in the context of work (direct perception) and learns through repeated use of affordances and effectivities (invariance). Mace (1977) captured the essence of an ecological-contextualistic worldview when he stated "ask not what is inside your head but what your head is inside of". Problems can be seen as exercising opportunities as specified by information in the environment if one has the correct effectivities to act on the affordance when it exists. This places problem solving clearly within an ecological "situated cognition" perspective (Brown et al. 1989; Young and McNeese 1995). Hutchins (1995) is representative of a similar perspective termed "distributed cognition" which is indicative of how cognition forms in context, and provides the foundation that cyber security activities can be wholistically framed as distributed cyber cognition.

Distributed cognition is heavily coupled to perceiving change in the contextual environment that specifies information. Therein, most of these approaches emphasize the role of perception, perceptual differentiation, and the ability of people to understand what that change represents in cyber-worlds in terms of transactions necessary for the agent to accomplish intentions. Perceptual apparatus is bound to the body (e.g., eyes, ears, limbs) – termed embodied cognition (Wilson 2002) – and is the basis for dynamically moving through and experiencing the context as it unfolds. Cooke et al. (2013) has adapted similar ideas as applicable to interactive team cognition providing an ecological basis for team activities especially as pertinent to cyber security applications. Likewise, McNeese (1986) first used the terms macrocognition and

macroawareness to describe cognitive activities that are broadly defined and interactive with the natural environment. More recently Klein et al. (2003) and others have extended macrocognition theory as a basis to understand and design solutions to naturalistic decision making problems that are present in many fields of practice. The worldview that this chapter takes is closely aligned with these approaches for individual, team, and 'team of teams' activities, rather than older more traditional perspectives of cognition.

When perception in and of itself cannot pickup information specification directly from the environment, then a person's own cognition and in particular meta-cognition (thinking about thinking) come more into play to make sense of and respond to situations. The environments that are meaningful for success also include social transactions that are distributed within a team or across teams, therein ecological contextualistic worldviews necessarily gravitate towards social connectedness and virtual transactions where information specification in teams is prevalent (or could be prevalent).

The meaning of awareness. As researchers who have historically focused on socio-ecological development of cognitive technologies it is incumbent to ponder what situation awareness or awareness represents in the cyber security/cyber defense field of practice. Some believe that answers will be found when there is an increase in the capacity in data accessibility. Others suggest awareness comes through "intelligence" built into computer algorithms or by reducing uncertainty via probabilistic or machine learning computation. Concomitantly, other worldviews suggest that improvements in awareness come through visualization, visual analytic displays, or through the massive amounts of information that are hidden in "big data" waiting to be data mined. Other perspectives – if even considered – place awareness solely in the mind through consideration of attention and memory activation processes (traditional cognition). More recently, researchers have suggested awareness emerges out of the team mind (Salas et al. 2012). While our work has touched on each of these perspectives at some point across the last six years of our Army Research Office ARO MURI grant; each one considered in isolation is significantly lacking as it fails to portray the big picture, see McNeese et al. (2006), (or what some refer to as the Common Operational Picture of Cyber Situation Awareness in Security).

There are multiple kinds of awareness present in socio-cyber systems, emergent across time and space, represented in various ways to human and agent; distributed across cognition. This is our collective view of what awareness means within cyber worlds. Hence, we refer to this niche as Cyber Distributed Cognition. Based on our own work the following elements are considered primary research missions within this niche:

I. Opportunistic Problem Solving in Cyber Operations
II. MetaCognitive Reflections about the Threat
III. Learning and Spontaneous Access of Knowledge in Context

These missions are both interactive and iterative with each other holistically. Because we believe that cyber situation awareness is an immersive, evolving state that

draws from cognition into the context as opposed to merely static knowledge state in the head, our missions point to different ways of thinking about awareness as it plays out within cyber distributed cognition. The missions also formulate some of the backbone of discovery that underlie our actual research objectives during the course of the MURI grant.

Cyber security operations can be punctuated with changing events, volumetric data exchange, and rife with uncertain circumstances. While many procedures are straightforward and known new data can flow into the environment, which causes assessment and awareness to be a high priority. This kind of environment presents the human analyst with ample opportunity (but with associated risks) to engage in opportunistic problem solving (Hayes-Roth and Hayes-Roth 1979). Cyber-worlds can also be nuanced in different ways wherein there may high levels of interdependence, overlapping layers, distributed information, and other forms of isomorphism. Yet it is frequently the case that individual analysts may have their attention diverted into a black hole of exploration and discovery when they are engaged in sensemaking and putting together patterns to determine affordances and effectivities. This presents a kind of bias that is opposition to collaboration. This may be especially true when individual analysts are not in the same physical locale, that is, when they are distributed. Opportunities for collective induction (Laughlin 1999) may exist but knowledge may remain hidden and not shared for maximum utilization (see Stasser and Titus 1985). In cases such as this unique knowledge may remain hidden and inaccessible by other analysts who actually could use it connect the dots to form the big picture. When collective induction is limited, then opportunistic problem solving may suffer and in turn solutions may be minimalistic or not produced at all. If collaboration involves integrative roles wherein distributed information is linked in cyber operations (as it often can be) then a more deleterious effect can occur especially if the distributed information has temporal contingencies and consequences associated with it.

The individual or team of analysts do not just come to a problem or situation without any experience. Typically, they will be place on the job with some level of training and in various circumstances analysts fall on the continuum between novice and expert. As part of their experience, learning is very important as it exposes an analyst to varying situations that may hold some degree of similarity or common elements where previous knowledge can be automatically (spontaneously) accessed and used opportunistically in the midst of a problem. This type of information may be specified directly through perceptual pickup wherein the analyst or team of analysts recognize cues that heed access to cases, stories, or segments of previous experience. Understanding by stories or cases or segments may rely upon metacognitive activities in that analysts may see something that reminds them about how they solved a similar situation in the past. Thinking about how they think is termed metacognitive activity and can occur at anytime but especially is salient when perceptual pickup stirs partial recognition.

Without awareness in cyber distributed cognition, an analyst can have a dim perception and consequently lack a basis for how to adapt or respond to a situation that involves cyber activities. We refer to this kind of state as mindlessness, in contrast to mindfulness. When situations are ill-defined, non-routine, and uncertain it can produce a state akin to “blooming, buzzing confusion” (James 1981) wherein there is a fuzzy

fog and focus is sparse. It may be experienced from several sources such as; (1) not paying attention to primary and secondary cues within the environment wherein recognition-primed decision making (Klein 1999) is lacking, (2) information overloading is experienced wherein focus is scattered, (3) stress or affective levels shuts down the neurological apparatus, or (4) time pressure requires a very fast response. When two or more of these sources combine simultaneously an analyst may devolve into what we refer to as cogminutia fragmentosa (McNeese and Vidulich 2002) whereupon attention is channelized into small strands, and is perceived in piecemeal fashion, and mindfulness is never obtained. If this happens during a live event then mistakes, errors, or even failure can be eminent. Therein, a cyber-world should facilitate human centered interaction to prevent mindlessness and facilitate mindfulness in order that awareness might evolve to high levels.

Framing the Problem Space – Use of the Living Laboratory (LLF). As mentioned one's worldview can intimately determine what is a problem and what is not a problem dependent on a researcher's perspective. Because we view cyber SA as distributed, cognitive work that is mutually influenced and effected by the context of action it is incumbent to utilize our own Living Laboratory Framework –LLF- (McNeese 1996) to discover and explore problems within cyber distributed cognition. Figure 1 shows the Living Lab Framework. We utilize the interdisciplinary framework to conduct research through multiple levels of analysis and design. The framework emphasizes the mutual relationships and cyclic nature of theoretical and practical constraints of work. The Living lab emphasizes the idea of exploring real world contexts by understanding worker or team-centered problems that emerge during complex operations. This is an

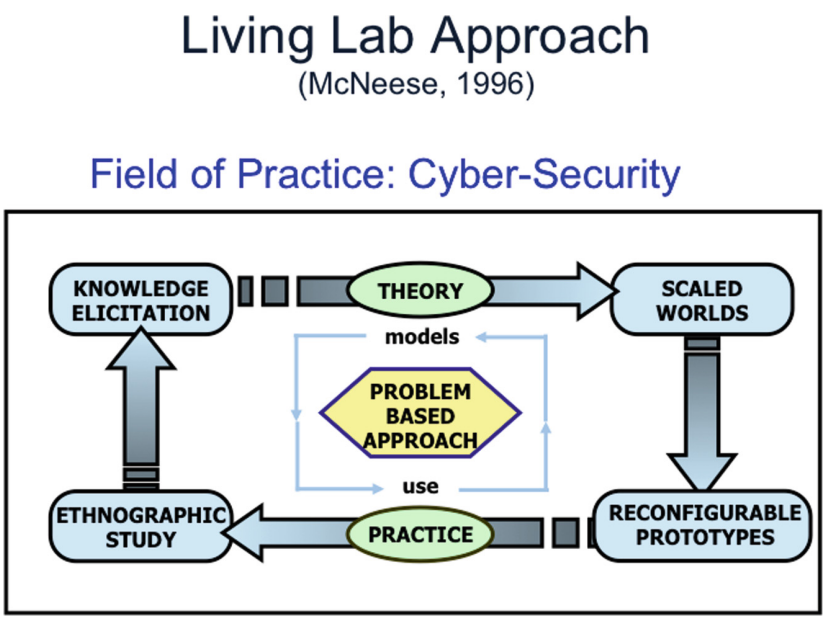

Fig. 1. The living laboratory framework

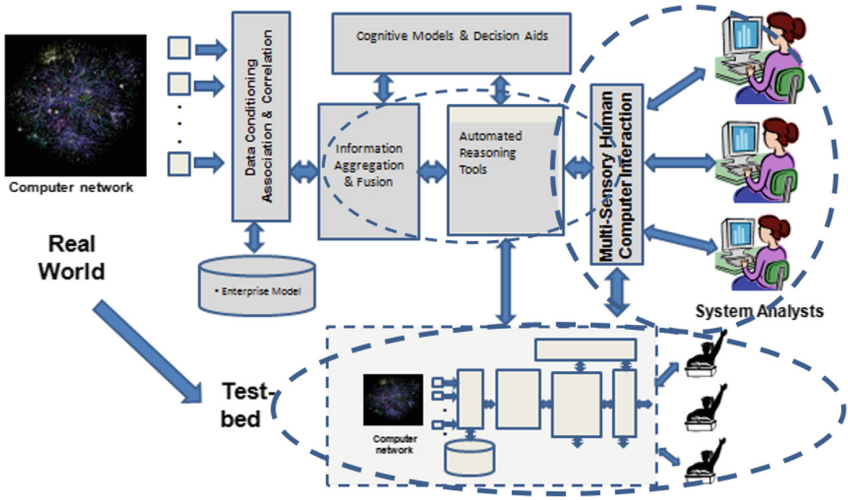

Fig. 2. Instantiation of LLF for Cyber SA MURI Grant

approach that is reflective of the ecological-contextualistic worldview. It has been classified previously as a cognitive systems engineering methodological framework (McNeese and Vidulich 2002). Figure 2 shows a more specified instantiation of the LLF as we utilized it for the MURI grant.

As one can see the central heart of the framework is that of discovering - defining – exploring problems to learn new ways of solving problems. Clearly this framework then enables a problem-based learning (Bransford et al. 1999) approach to human centered cyber SA. Problems come into focus through a variety of means. This is captured in the framework by the interactions of the four elements: (1) ethnography, (2) knowledge elicitation, (3) scaled world simulations, and (4) reconfigurable prototypes. Problems can be informed from the top-down -through theoretical positions- and from the bottom-up - through practice. Practice in the real world as we know is coupled to extant problems that occur as users experience them in differing ways. This excites the bottom-up processes in the LLF that focus on what gets done in cyber security (in particular, cyber situation awareness) and how people utilize technology to accomplish work. As related earlier much of this work is distributed and complex. Concomitantly, problems are also coupled with theory or theoretical positions taken by researchers.

Theory provides a view of what could happen in cyber security by postulating hypotheses about how human-cognitive agents transform their world. Because our worldview necessarily incorporates human-in-the-loop processing of cyber security, practice is typically known (heeded) by the experience that an agent (analyst, operator, or user) encounters while involved with distributed work. At the core of the LLH then is the coupling of theory-problems-practice and the ways they are informed by feedback from the four elements that can provide additional enhancements of data/information/knowledge. As learning ensues in a given element it feeds-forward to setup processes in other elements as well, and also improves comprehension. Research coupling among these elements also may yield secondary increases regarding use and

modeling. By cycling though these elements the framework affords a living ecosystem approach to distributed, cognitive work that promotes an interdisciplinary, transformative, systems-level thinking in advancing success in cyber-worlds. We will return to unpack this figure with more specificity as we get into the specific activities of our MURI research a bit further along in the chapter.

Engaging the Problem Space – Distributed, Cognitive Work. We begin by reviewing some of the attributes we know about the problem space. Our framing of the problem is best taken as 'situating cyber situation awareness' paper (McNeese et al. 2011) developed directly from our MURI work. That paper enabled a distinctive cognitive engineering perspective to understanding cyber-worlds, which has continued in our research throughout the grant. So the first premise is that awareness within cyber worlds is work that engages cognition within specified contexts wherein technology developments improve aspects of sense-making, decision making, problem solving, and/or action potential.

This coincides with a human centered approach where cyber security is viewed as first and foremost as distributed, cognitive work wherein tools and technologies support cognitive work to improve performance (eliminating problems, enhancing capabilities, removing constraints, adapting response). Taking that as our baseline, lets delve in more depth as to what this means. The attributes we find embedded with the cyber security world embroil around difficulties humans have as agents engaged with a complex context. Figure 3 summarizes these problem attributes on a general level and the consequences that emerge for humans.

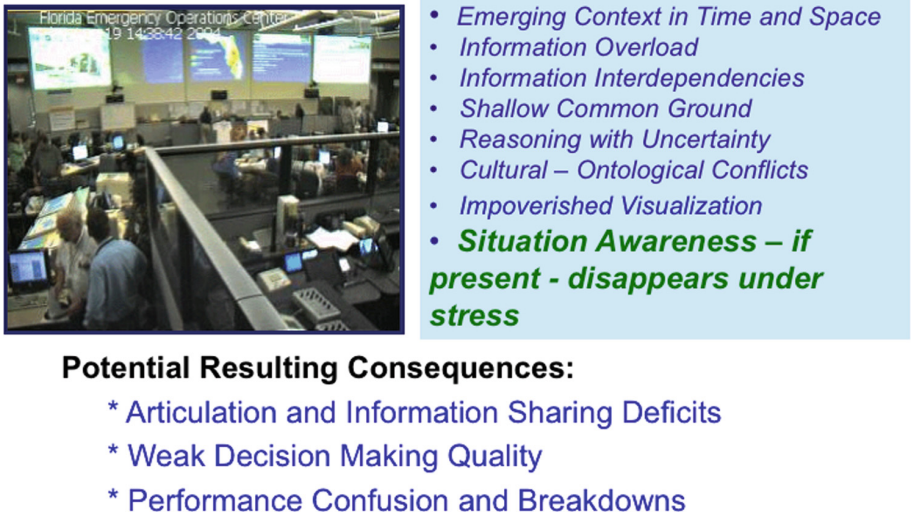

Fig. 3. Problems encountered in distributed work settings

Exploring Cyber Distributed Cognition Using the Living Lab Framework
Considering the above problems and issues that are pertinent within cyber security operations, there are three specific areas (premises) we wish to look at:

(1) Cyber-situation awareness as distributed cognitive work as performed in a given context, field of practice,
(2) Cognitive work will focus on human-systems integration centered on information fusion for both hard and soft sensor data,
(3) Cyber operations potential can improve with apropos teamwork (both within and across team performance).

Given that our theoretical approach within the Living Lab Framework is distributed cognition and given we have defined what some of the problems are in practice, we will now look at other components of the framework that have been explored the last several years: (1) knowledge elicitation, (2) ethnographic exploration, (3) scaled world developments, and (4) prototype technologies. The LLF is not pre-specified in a linear, assumed order but rather is adaptable to the circumstances the researcher must work within. This chapter reviews outcomes associated with distributed cyber security, socio-cyber systems, and awareness by summarizing accomplishments within two distinctive but related trajectories: qualitative research and quantitative research. Both of these trajectories as part of the LLF are mutually informative and provide feedback cycles to further 'knowledge as design' as more results become available. While there are multiple research accomplishments within each track this chapter focuses on recent work. We begin with qualitative research.

3 Qualitative Research: Knowledge Elicitation/Ethnographic Data

One of the challenges for research in cyber-security is the access problem of experts. Unfortunately, much of the work in cyber security operations is classified and therein unattainable. To overcome this early in the MURI we were able to; (1) participate in a workshop at Arizona State University with some cyber analysts who provided invaluable information to general levels of thinking about cyber analyst work and what situation awareness amounted to –from their experiences, (2) interview/observe different kinds of cyber analysts from different venues (university, business) and in a war game exercise, (3) collect results from a survey given to 112 cyber security experts, and (4) conducted interviews from students from our College who were participants in a recent student regional cyber security exercise. In addition, we had the benefit of faculty members who had prior professional experience and cyber/network analysts.

Through our various contacts we have derived early ideas about cyber work and further elaborated the spectrum of problems that are extant and relevant. We have previously published aspects of # 1, 2, and 3 above (Tyworth et al. 2013) so will not reiterate everything mentioned there. Many of the problems mentioned earlier in the introduction are present in cyber activities, and we have discovered from triangulating across these sources of data that cyber security: (a) involves a hidden – often ill-defined

threats, (b) takes place in a notational environment with much context switching present, (c) location and spatial cognition is emphasized (thinking about space in the computer is different than physical space), (d) representation of locations (where cyber attacks occur) especially with temporal constraints is often a problem (this motivated our development of a visual analytics workbench), (e) tracking of problems-situations range from location-time-space representations translatable into semantic descriptions (data-information-sensor translations), (f) there is often collaborative and intuitive reasoning preset wherein human and machine tools related to situation awareness may be most useful), (g) more data is not necessarily useful as it can produce overload and obfuscates comprehension, (h) tools are not very good – they do not deliver what was promised (often this has to do with scale up problem), (i) having to reason and process more information can result in fatigue and burnout (which contributes to mindlessness), and (j) there is often isolation – no common ground present and therein collaborative problem solving is not really supported in any effective way.

We discovered that implications associated with awareness - given these problems – are important. Situation awareness can come and go dependent on what information is known or unknown at a given point in time and this acts as hidden knowledge across team members in the team setting. As complexities grow the focus of intentions can become blurred, disjointed, and channelized (more evidence of mindlessness in operation). Understanding attacks can be confusing when SA comes and goes and when these attacks are multiple and distributed over time. While there are more insights discovered that represent some of the main findings, this qualitative section focuses more on the recent qualitative study with students. (See Tyworth et al. (2013) for more information regarding other qualitative work that imbues individual and team-based distributed cyber cognition.)

Regional Student Competition. One of the primary objectives for recent work in cyber distributed cognition was focused one the use of a Cyber Threat regional exercise which our SRA students participated in as student teams. This objective represents more of a need for qualitative data directly taken in the form of knowledge elicitation interviews, which can then be used to propagate initial concept map-based models.

Preparations and Development. We were given an opportunity to have access to a College of Information Sciences and Technology Security Club project wherein members competed in the Mid Atlantic Collegiate Cyber Defense Competition. This allowed us as researchers to develop a qualitative study to determine how they would problem solve and make decisions when presented with an engaging Cyber Security Threat Situation. As part of the competition they were asked to participate in a challenge problem.

Challenge Problem. The following paragraph describes what they did on the challenge problem in the regional competition:

The work they performed was typical cyber-defense activities. They were given remote access to two Linux and two Windows-based servers to defend from live “red-team” attackers. They were also provided dynamic injects of tasks they were asked to perform – typical systems administration tasks, account creation, database updates, etc. They had full administrative access to the systems they were defending, so they could do anything they wanted. Typical

tasks included enumerating and securing accounts with administrative access (changing from default passwords), identifying and updating software with patches, modifying configuration of software to turn off unneeded services, etc. During the exercise, the students needed to identify what was wrong (configuration, patches accounts, services), figure out if attackers were utilizing those vulnerabilities to compromise systems, and turn off attacker access if they were able to locate that the attacker had gained access.

Methods. The participants for the qualitative study were recruited from the team of students that were participating in the National Collegiate Cyber Defense Competition (CCDC). After the project was described to students. Informed consent forms were signed, and the participants were questioned about their team experiences, training and preparation activities, and understanding of the competition and their teammates. The interviews were recorded and notes were also taken to supplement the digital recordings.

When all of the interviews were completed, the digital recordings were sent to a transcription service that transcribed the data word-for-word. In instances where the recording was inaudible the handwritten interviewer notes were used for clarification. All of this data was analyzed by two of the researchers collaboratively. Key phrases were pulled from the transcript and put into a spreadsheet. Once the key phrases were identified, the same researchers worked together to identify themes and categories in order to create the coding scheme (see Table 1). This coding scheme was again collaboratively used to classify each of the key phrases previously identified. In cases in which a classification did not exist, the coding scheme was modified and the process continued as normal.

Results. The outcome of the coding scheme application resulted in specific frequency of occurrence of codes across all interviews. This highlights the nature of distributed cognition, situation awareness, and individual and team cognition as it relates to students identifying, exploring, and solving the challenge problem(s).

In addition to understanding the content of the entire set of interviews vis-à-vis the coding scheme, a plan was derived to produce a descriptive model of the student's distributed cognition to ascertain how situation awareness emerged within knowledge, context, and process. The use of concept mapping (Zaff et al. 1993) was chosen as a flexible, lightweight kind of cognitive model and was collaboratively formulated by the same researchers who coded the interviews - by utilizing the raw text of the interviews and the frequency occurrence produced by the results of the coding scheme. An overall plan was generated to produce an integrative, overlay model of cognition (see Fig. 4).

To initiate this plan, the first phase accomplished included creating a declarative concept map to represent some of the major findings in the coding scheme (as applicable to the actual interview text phrases) to come up with a first-level model of knowledge underlying distributed cognition in cyber operations teamwork. The declarative concept map in turn represents element # 1 in the overall overlay: *intention.* The other elements (*solution path*, *teamwork in evidence*, *cognitive processes demonstrated*) would also need to be developed to completely in the next phase of future work to completely propagate the entire overlay cognitive model. The first phase model (see Fig. 4) is heavily informed by the activity of planning and re-planning, and determining what role uncertainty plays in accomplishing the overall challenge problem. As we perused this initial concept map there was much to be learned in how

Table 1. Coding scheme used to analyze interviews

4	**Problem Solving**	Activities necessary for identifying, addressing, and resolving issues
4.1.	*Strategies plan of action*	
4.1.1.	Shared across the team	
4.1.2.	Individual strategies	
4.2.	*Processes*	Articulated written or unwritten plans necessary to address problems
4.2.1.	*Actual*	What were some of the processes of problem solving
4.2.2.	*Adaptive*	Flexibility of processes when new information was presented or something was found to not work
4.3.	*Problem Monitoring*	Activities and techniques for tracking and documenting problems
4.3.1.	Initial identifications of problem	
4.3.2.	Updating problem	
4.4.	*Process Monitoring*	Tracking and documenting of the processes for problem solving
4.4.1.	*Strategies*	is there monitoring of those actions used to problem solve
4.4.2.	*Outcomes*	are the results desired or appropriate to the task
4.5.	*Reassessment*	
4.6.	*Errors*	What happened when there were errors?
4.7.	*Tools*	
4.7.1.	Information Technologies	
4.8	Priorities	
4.8.1	Updates to	
5	**Planning**	Activities for the purpose of having the necessary skills, personnel, and knowledge to be successful
5.1	*Team based planning*	Activities coordinated among the team for planning purposes

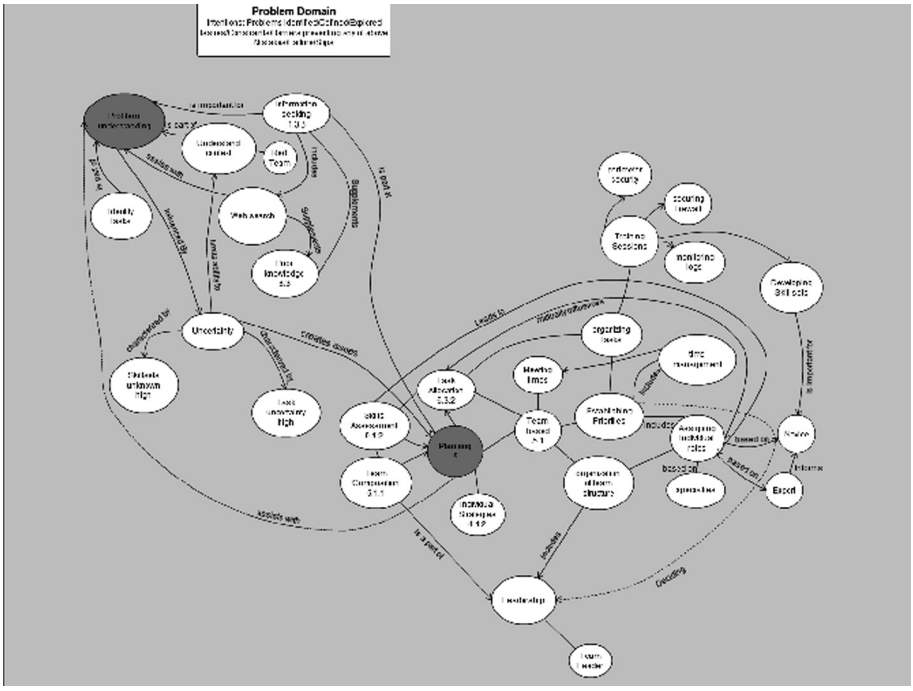

Fig. 4. Declarative concept map of intentions-solution paths

individuals and teams formulate what the challenge problem consists of, and in turn how to begin tackling it. All of this is valuable for understanding comprehension of cyber threat activity, and how this might be improved with new cognitive technologies that would enable information fusion and potential gains through collaborative teamwork.

Implications. It is evident that students working together in teams often struggle to understand how they will solve the problem given to them and how they can work together to reap the benefit of their collective talents. In newly formed teams this is difficult process as it minces strategic knowledge resident in teamwork processes with specific knowledge needed to solve the problem at hand.

Furthermore, the management of their intentions becomes a reified issue in that they have to spend time figuring how to work as individuals but yet as an interactive team, including defining "function allocation" (i.e. Who will do what when with what tools?). Although this was a first-level concept map specifically focused more on planning – it is the first of several concept maps that could be generated as part of the layered representation.

4 Quantitative Research: Simulations, Design Prototypes and Experiments

Much of the work within this trajectory is interrelated as we often design scaled worlds (and the scenarios within) as human in the loop simulations to address specific research problems-issues-constraints initially revealed by novices and/or experts engaged in specific problem spaces (e.g., novice Security and Risk Analysis (SRA) students engaged in the Mid-Central Regional Exercise as reported in the previous qualitative work section). So at the most fundamental level scaled worlds have been designed to take broad problem spaces that exist in practice and scale them down into experimentally tractable simulations that are can be controlled and manipulated according to objectives. The goal is to have an experimental simulation that represents many of the elements of the cyber operations context (such that it appears as a real work environment) but is adaptable for testing and evaluation purposes. To that end, most of our simulations-scenarios are adapted for either testing the theory-based understanding (distributed cyber cognition and awareness) or for evaluating the intervention of an innovative prototype within the scaled world (socio-cyber systems) to see if it influences individual or team performance. Once a prototype is tested and design to the point it positively influences performance in the scaled world, then it is at the state of readiness for application within the real world context it was designed for. If the LLF has evolved technologies to this point they are then inserted into the real world context for actual application testing and the cycle of understanding begins again. At this point we have not actually placed prototypes into actual practice as they still need further testing under different conditions.

The simulations are absolutely designed from our worldview in the sense that they represent human-environment transactions and are strongly ecologically contextualistic. The transactions needed occur when some form of 'change of state' emerges from

the context which requires a human to perform in a certain way to cause positive change in addressing problems-plans-subproblems-outcomes. Indeed, all of the simulations we have designed represent changes in the cognitive-contexual continua that a person or team must contend with. Affordances for action are created based on emerging events that create changes in various states which can then be resolved by application of different types and amounts of resources (effectivities). Certain team roles restrict who may do what at what time but together this syntax creates complexity representative of real world cyber situations that are often time-based. Awareness comes from comprehending the emergent situation based on assessment of events within situations, and how well resources are producing positive effects in resolving events. The development of socio-cyber systems often springs off of developing new technologies that specify information about an affordance to make it more visible or known, extending the conditions under which an effectivity is appropriate, advancing awareness based on expectations of state changes, and sharing of hidden knowledge to create a bigger imprint of the common operational picture at any point in time. Tasks can require analytical inquiry at the individual level but also may demand information sharing and collective induction. By simulating real world events and simulations much can be known that was not previously considered. This brings forth 'knowledge as design' and generates new ideas and concepts that are relevant to cyber security concerns.

The simulations have built in dependent measures that accumulate the degree to which performance approaches the optical level based on how well individuals or teams resolve the total number of situations-events that occur in the simulation, and to what degree or level they were resolved to. These simulations require comprehension of the problem, awareness of changes that emerge, communications with team members about all aspects of what is going on, and a lot of individual work representative of a particular role they are responsible for. Because the simulations often present dynamic occurring cyber events, the best-laid plans have to be refigured and revised. This emulates the necessity for replanning which is often one of the bugaboos experienced in complexity and problem solving. When replanning is successful human-environment transactions make headway and problems dissipate. In many cases, the distributed social interdependencies are the most important considerations to pay attention to (i.e., where cyber awareness develops and comes into play as to whether performance will increase or decrease) as they create uncertainty, analytical reasoning, are heavily dependent on temporal awareness. The simulation design affords implementation of actual experiments wherein experimental independent variables are manipulated to see the effect upon dependent variables. The simulations in general also manage control variables that are necessary so as not introduce new extraneous variance. Often as mentioned above scaled world simulations tests a given hypothesis derived from the theory under examination, but it can also test different states of a new technology to see how it might interact with other experimental variables as part of an overall study. Therein, the scaled worlds, experiments, and technology prototypes are intimately coupled together for evaluating ideas and concepts within a domain that represents the real world problem specifications.

Specific Cyber Simulations Developed. During the first four years of the MURI grant one of the focus areas was to specify, create, and build simulations that would emulate salient elements of (1) cyber distributed cognition (2) cyber situation awareness (3) innovations in socio-cyber systems. The goal for these simulations was to provide some degree of flexible experimental control that would impact scenario design generation and to provide quantitative testbeds that could be activated for specific human in the loop experiments. In turn we achieved our goals by developing 3 specific scaled world simulators (1) CyberCITIES (2) TeamNETS (3) IdsNETS (4) NETS Dart. The CyberCITIES simulation was our first simulator in the cyber area and the task focused on recognizing and utilizing information surrounding access control within cyber security (Reifers 2010). Because these simulators have been reported and described elsewhere we will not dwell on them here, Tyworth et al. (2013). By all accounts they were successful as providing adequate experiences with different aspects of cyber security operations albeit with certain constraints and assumptions. One of the essential issues for all the simulations is determining how much training to provide for students. Actually the topic of training and learning is an area the simulations might be extended, as training over time produces insights, expertise, and awareness that was not present previously. This argues for actually conducting longitudinal studies that emphasize the learning of metacognitive activities, spontaneous access of knowledge when it is needed, and how to operate and integrate knowledge effectively as a team. While most experiments focus on single shot studies (one and done) it is our belief that the LLF is best implemented when longitudinal simulations are invoked.

All of the simulations focused on both individual and team cognition requirements within an emerging scenario design in which different events had to be assessed and processed with some rigor. These simulations absolutely required interdependencies across the information-role-context coupling, and all of the simulations represented analytical thinking requirements and the need to communicate with teammates in order to obtain acceptable scores. The simulations also provided a 2-way testbed where the outputs from qualitative research could be a basis for developing a scenario that was grounded in reality. Although each of these simulations had limits as to what could be done – they provided a basis for generating situation awareness and situated action within a specified cyber distributed cognition context. Likewise, the simulations were designed so that new prototypes could be configured within the simulation. This enabled human in the loop testing of new innovations, which could be compared with control cases, as well as salient experimental variables that represent some of the problem states and issues we identified earlier (e.g., time pressure).

The simulations are all predicated on client-server technologies wherein command and control are achieved vis-à-vis experimenter's stations. The picture in Fig. 5 shows the laboratory setups of some of the simulations. Individual stations are shown on the top and bottom figures (enabling experiments to be conducted in which participants act as individuals, members of a closely linked and interacting team, or members of a pseudo distributed team environment.) The middle picture of Fig. 5 shows our Extreme Events Laboratory which supports 3-D visualization experiments, utilization of 3-D sound (i.e., experiments with sonified data interaction) and combined visualization/sonification interactions.

Simulations were designed to absolutely be distributed in the sense that they could provide distributed space (team members are connected via interfaces and chat rooms but remotely located from each other), distributed information (information has to be fused together at individual and team levels to address task demands), and distributed context (in some simulations context switching must occur which challenges awareness).

Human in the Loop Experimental Studies

As part of the nexus between theory-problems-technology feedback loop within the LLF we have utilized this set of simulations for experiments that help to inform and understand cyber distributed cognition in general and how awareness evolves within socio-cyber systems in particular. The goal of human in the loop experiments is to test individual and team cognition under variously constrained conditions to evaluated theoretical perspectives, hypotheses that aim to discover new possibilities in opportunistic problem solving, and to develop and test innovative solutions to problems that are difficult. The set of experiments we have designed and implemented are a mere subset of what is possible to look at given the simulation capabilities, but are the ones we have data on to date. These studies taken as a whole demonstrate that cognition-context-communications-computation-teamwork all play roles in successful problem solving to varying degrees. The design, implementation, and evaluations we produced using the Team NETS, Ids-NETS, and DART NETS simulations have been previously described in Tyworth et al. (2013) but are captured here to provide additional edification as to how our new simulations can be used. The following exert describes experiments that were undertaken to further the understanding of cognitive science within cyber operations:

> "We have conducted experiments using the scaled- world simulations. One set of experiments examines transactive memory and CDA. To conduct these experiments, we have updated NeoCITIES scaled-world simulation (c.f., Jones, McNeese, Connors, Jefferson, & Hall, 2004; McNeese et al. 2006) to better support the dynamic and rich nature of the cyber security environment. The new simulation, the NeoCITIES Experimental Task Simulation (NETS), has been extended to support richer scenarios and complex decision making. The current implementation of NETS (referred to as idsNETS) has been implemented using intrusion detection data to mimic the role of an intrusion detection analyst. We have plans to extend the NETS functionality to be able to simulate scenarios from the other operational domains we identify in the future.
>
> For our own research, we are addressing the issue of the formation and maintenance of transactive memory systems in synchronous distributed collaborations. To study this, a new version of the NETS simulation was designed (teamNETS) to simulate collaborative problem solving tasks within a cyber-environment. This version of the simulation was extended with numerous enhancements to better support our research questions and transactive memory research at large. Within the study, each team member is assigned a particular specialty, and in order to achieve high performance, it is necessary that they communicate and share relevant information to solve different types of events. From this study we hope to gain an understanding of how these transactive memory systems are formed in distributed collaborations, and how new systems can be designed to better support this process.
>
> Transactive Memory was first conceptualized by Wegner (Wegner 1986) as an "interpersonal awareness of others' knowledge" and can be conceptualized as a specialized form of Cyber Situation Awareness, where rather than focusing on, or being aware of, aspects within the cyber environment, your awareness is grounded in the cyber knowledge, activities and behaviors of your collaborators. An effective Transactive Memory System can give a human quick and coordinated access to another person's specialized expertise (Lewis 2004). Numerous

Fig. 5. Laboratory environments for cyber operations

studies have shown a positive link between a team's Transactive Memory System and its performance in collaborative tasks (c.f., Ellis 2006; Moreland and Myaskovsky 2000; Pearsall and Ellis 2006).

Whereas Transactive Memory is an important thread within team research it is mainly approached from a management or organization psychology lens, often only considering the humans. Since its inception, technology and information have evolved dramatically, though Transactive Memory has remained fairly constant. Research has focused primarily on exploring its effect in new domains, and extending the concept as a research tool, but no one has examined how new technologies have changed how we, as humans use this transactive memory. In order to bring Transactive Memory into the 21st century, it is imperative that we understand how transactive memory has changed with synchronous distributed collaboration systems, social networks, and crowd-sourced knowledge repositories, to name a few.

A second set of experiments is being conducted to look at the impact of task load on the ability of participants to establish and maintain cyber-SA and prioritize tasks. Maintaining cyber SA is, in part, dependent on the ability to prioritize attention. Cyber defense analysts must attend to alerts associated to potential threats and respond to them within time constraints, requiring a prioritization of events in accordance to their threat level. However, high levels of cognitive workload may limit the ability of analysts to focus their attention on priority tasks. For example, unexpected surges in threat level in some events may not get noticed in time. An interface that provides information on anticipated threat level could facilitate analysts' ability to attend to unexpected surges.

In this set of experiments, we explore the effect of a workload-preview on performance in a dual-task cyber- security event monitoring context using our NETS-DART scaled-world simulation. The simulation provides a dual- task environment. The primary and secondary tasks represent internal and external networks in an organization. All participants are presented with two types of scenarios – regular scenarios and surge scenarios. The difference between the two is that surge scenarios consist of secondary-task events that grow in threat-level and exceed that of concurrent primary-task events. Experimental results are expected to provide insight on the effect that workload previews have on attention- allocation, task management and cyber-SA in multi-task cyber-security contexts. (pp. 8–9)"

After completing the previous simulations (TeamNETS, IdsNETS, and DART NETS), we embarked on the development and test of simulation designed to be strongly linked to actual cyber security operations. This resulted in the newest and most current development of a scaled world simulation termed Cybernetic Team Simulation (CYNETS). The following section describes ongoing work that led to CYNETS becoming a reality.

CYNETS Simulator Proof of Concept. At this point in the chapter we turn now to the most recent proof of concept simulation that was designed, CYNETS.

Preparations and Development. Inherent in our simulation – CYNETS - was the desire to create scenarios that built off of realistic hard data to provide a solid scaled world feel wherein the collective demands on distributed teams would be bound to both hard and soft data integration. Also, we desired a simulator with a scenario that required discovery-information seeking, team communication/coordination, cognitive processing, and therein a task that was ill/defined and uncertain to a degree that would enable the necessity of developing cyber SA.

CYNETS Task. The work they performed was typical cyber-defense activities. They were given remote access to two Linux and two Windows-based servers to defend from

live "red-team" attackers. They were also provided dynamic injects of tasks they were asked to perform – typical systems administration tasks, account creation, database updates, etc. They had full administrative access to the systems they were defending, so they could do anything they wanted. Typical tasks included enumerating and securing accounts with administrative access (changing from default passwords), identifying and updating software with patches, modifying configuration of software to turn off unneeded services, etc. During the exercise, the students needed to identify what was wrong (configuration, patches accounts, services), figure out if attackers were utilizing those vulnerabilities to compromise systems, and turn off attacker access if they were able to locate that the attacker had gained access.

Simulation Data. To develop hard data fusion elements, the experimental simulation data was created in the lab environment from a similar perspective. The simulated data was fabricated from a network of computers in the laboratory that simulates an active network of computers from a fictitious organization called "ABC" (see Fig. 6). The ABC network includes three servers and 25 workstations. The data that was provided to simulation exercise analysts included a 24-hour period of logon/logoff log data from a Windows 2012 server for the entire network.

In this 24-hour period, accounts were logged on and off of computer systems to create actual log entries in the Windows Security Log of the server. While the actual events of successful logon and logoff events are entered into the Security Log of the authentication server, these are not the only events that are generally displayed there. A windows domain treats computers in a similar way to the way it treats users. They must also log on and off. However, a systems authentication is more automated. Also,

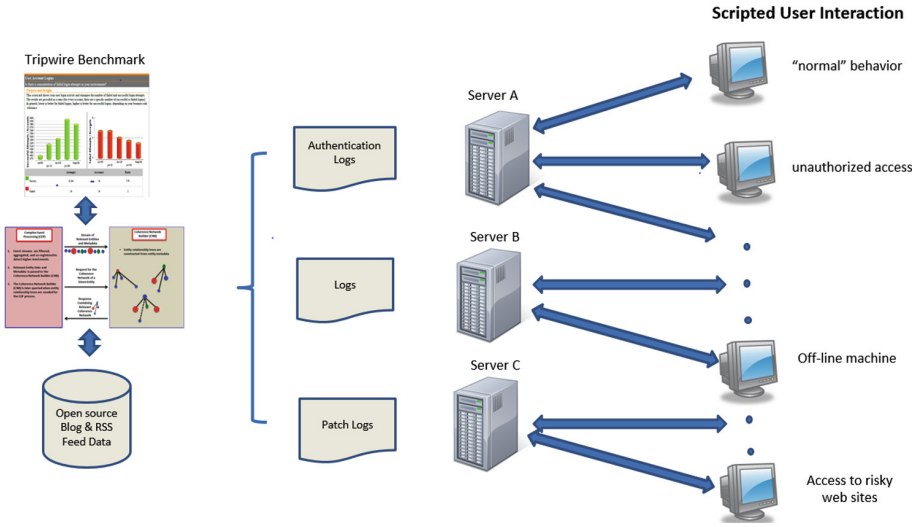

Fig. 6. ABC simulated network

as a user authenticates and accesses networked services, other authentication records are also in the log to include every time a networked user accesses a different network device. This noise of normal activity often clouds the real issues of authentication failure and account misuse. The data set that was presented to simulation participants had some level of normal noise, but generally was limited to successful logon, successful logoff and unsuccessful logon events. Embedded in the presented authentication data was a series of failed logon attempts, followed by an eventually successful event. This simulated a password-guessing activity that resulted in a compromised account.

Additionally, the same 24-hour period was used and a number of viruses were copied on to the computers. The antivirus program was allowed to detect these files and take appropriate action – either delete or quarantine the files with the malicious code. Together with the updates of new antivirus definitions, these two types of records were presented in the antivirus data. To simulate unsuccessful antivirus actions, anti-virus alerts were fabricated repetitively on one system. This mimics the behavior of some antivirus applications – where a suite of malware is installed on a system that re-installs other parts of the suite if they are removed. The undetected malware is indicated because of the repeating successful removal of several sets of other parts of the suite. Together with an outdated set of virus definitions, an analyst is led to the conclusion that the system must be infected with malware that is not detected by the old set of definitions.

The final set of data is patch management. In this case, we created a set of records of normally applied updates. However, we also intentionally left one system offline for a period to show the lack of updates being applied to that system. Additionally, we filled the hard drive of another system to prevent it from having patches applied. This system showed "failed updates", primarily because the drive was full. A network analyst seeing records from these systems would be able to interpret that the systems needed hands-on attention to figure out why they are not receiving their patches.

Methods. Three triad teams were recruited from an Information Sciences and Technology (IST) course within the College of Information Sciences and Technology (IST) at the Pennsylvania State University. Each individual was randomly assigned to one role for the simulation either (1) Windows Authentication Analyst (WAA), (2) Anti-Virus Analyst (AVA), or (3) Windows Update Analyst (WUA). Each role is responsible for reactionary machine and problem identification through the simulated logs as previously described.

Upon entering the lab and signing the informed consent forms, participants receive their randomly selected role and are given a pre-trial demographics survey. Subsequently, they are directed to read through a role-specific PowerPoint presentation for training. After all participants have completed the training presentation, a 5-minute training scenario is started to allow the participants to get familiar with the interface and the task. When the training scenario is finished, the participants are given a survey to quantify their individual situation awareness (SA) using NASA-TLX (Hart and Staveland 1988), SART (Taylor 1990) and MARS (Matthew and Beal 2002).

After the survey is completed, participants are given an additional training scenario followed by another individual SA survey. Following both training scenarios, the participants are given a quick debrief about the scenario and the proper response. Next, the first performance scenario is started and once complete is followed by the same

individual SA measures but with the added Shared SA Inventory (SSAI) (Schielzo et al. 2009). Subsequently, participants are asked to complete the second performance scenario and the same individual SA and SSAI surveys. Upon completion of the final survey, participants are debriefed about the fictitious nature of the scenarios and thanked for their service.

Results. The simulation was tested initially with 3 teams to assess feasibility and capture the performance measures mentioned above. Everything worked well in the simulation, and students were able to perform in the role of individual and team cyber analyst duties in determining routine and threat activities as part of their task. While the initial proof of concept was conceptualized, implemented, and tested- and met the expectations of the experimenters, more robust testing and experimentation is desirable. This is discussed further in the future work section below.

Implications. The CYNETS scaled world simulation represents the development of a challenging cyber operations environment that emulates real world threat assessment that involves distributed cognition across individual and teamwork functions. As such it provides a capability for extending understanding of hard (and potentially soft data fusion) within an emerging milieu. The implications are that the study of the problems mentioned at the beginning of this report can be brought into the lab setting and studied for further illumination of situation awareness within cyber defense. Further work on cognitive technologies that are human-centered in design can be embedded within the information architecture underlying the simulator designed to undergo precise human-in-the-loop testing to determine how they improve human/team performance.

Innovative Prototype Technologies

Visual Analytics Test-bench. During the research on the Multidisciplinary University Research Initiative (MURI) on cyber situation awareness, we conducted research on tools and visualization aids for cyber analysts. There are numerous visualizations that have been developed to aid the visualization and analysis of network systems (see for example Stall et al. (2014) and Shrvavi et al. (2011)). In particular, N. Giacobe (Giacobe (2015)) developed a prototype cyber analyst workbench illustrated in Fig. 7. The tool extends the typical concept of providing network-type displays (e.g., overlays of computer network topographies on geographical map displays, network "traffic" displays, attack maps, link diagrams, etc.), to include linking text-based data (e.g., cyber-network sensor data and reports on cyber-attack activities), with social network information (indicating potential threat perpetrators), timeline information, and ongoing analyst hypotheses and notes. The aim was to explore how a cyber-analyst might conduct situation assessment, analogous to the concepts of situation analysis performed by analysts for traditional non-cyber military operations. Indeed, Giacobe explored the applicability of the Joint Directors of Laboratories (JDL) data fusion process model for cyber security applications (Giacobe (2010)).

Complex Event Processing

In addition to visualization aids, research under the MURI grant explored automated tools to detect cyber events and activities. The concept of Complex Event Processing

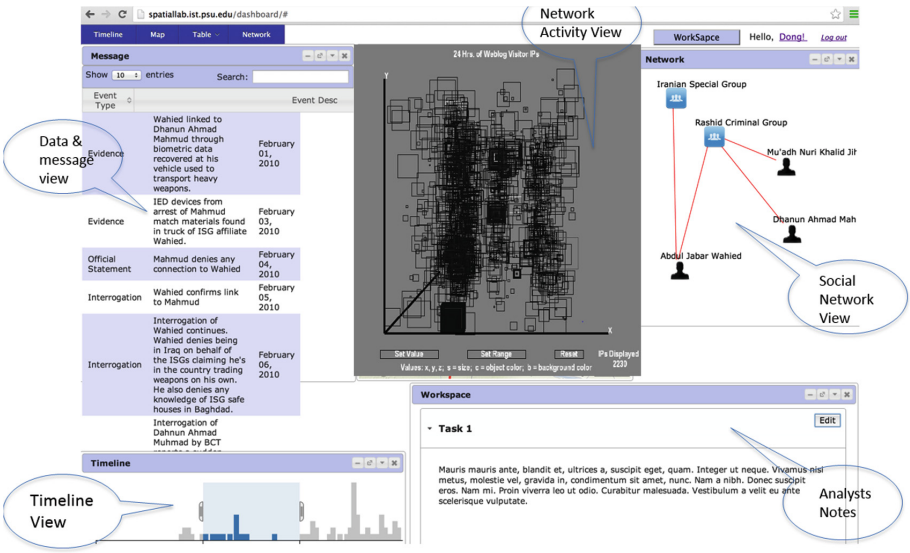

Fig. 7. Prototype analyst workbench (Giacobe (2013))

(CEP) has emerged from the business community and crisis management. The concept involves developing an explicit and implicit representation of conditions, observables, and contextual information that provide evidence for an emerging activity or event. Rimland and Ballora (2014) explored the application of CEP to detection of cyber-attacks. Their architectural approach is illustrated in Fig. 8. In addition to considering the CEP approach, they also explored the transformation of cyber data into sounds (sonification) in order to improve the interface with analysts (viz., transforming network conditions into sounds so that analysts could more readily detect anomalies).

Discussion/Future Work

The work undertaken represents further effort to open discovery, understanding, and prediction as to how situation awareness emerges in distributed cyber operations (both individually and in teamwork). While this is a lofty goal, the research described above (coupled with our five previous years of MURI research) has begun to make necessary in-roads in these areas. In particular, we have designed, implemented and provided an initial proof of concept for the CYNETS scaled world simulation involving distributed information fusion surrounding an emergent adversarial threat situation. While the first experimental design and test of the simulation only involved the incorporation of hard data fusion, the scaled world is designed to include soft data fusion in future studies to further extrapolate nuances of cyber situation awareness as cyber operations are employed in both routine and non-routine opportunistic problem solving sets.

Our use and testing of the scaled world using scenarios involving human-in-the-loop testing with Security and Risk Assessment (SRA) students within the College of Information Sciences and Technology validates that it is possible to create a realistic emulation of cyber security using typical data expressions and use from day-to-day

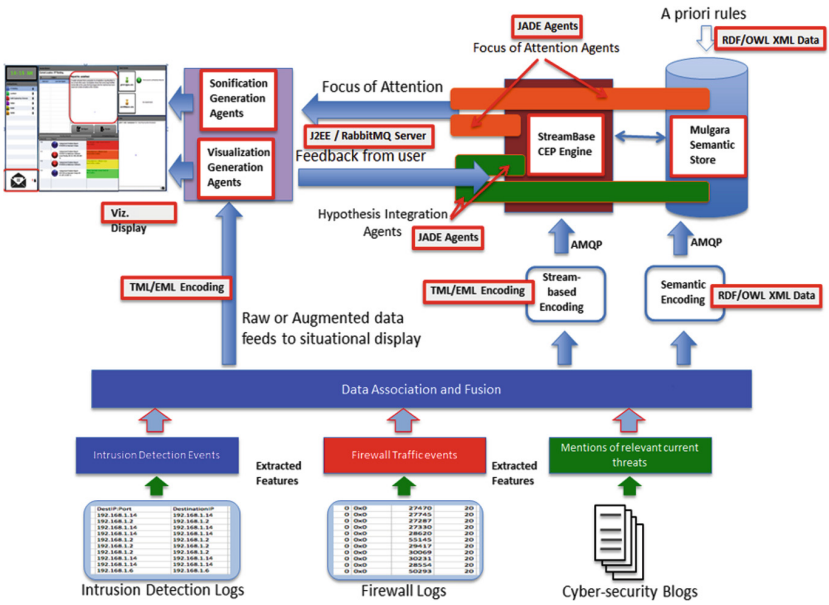

Fig. 8. CEP processing architecture for cyber SA

cyber analyst activities. The simulation affords analysis of individual cognitive processing as well as team cognitive processes to comprehend and discover specific problems and issues that arrive in predicting correct answers or solvation of complex problems. Having the availability of this type of simulation gives an additional tool to breakdown the reasons for individuals and teams not coming up with the absolute correct answers. This purports a "failure-driven learning" approach wherein over time correct answers may be discovered through use and interaction.

Concomitantly, it gives an ability to assess and analyze why wrong answers or procedures occurred potentially giving rise to detect and isolate bugs in cognitive models, and/or barriers to learning how cyber situation awareness comes into existence. Learning why SA does not envelop in the individual and in turn the group provides the basis upon which human-centered cognitive technologies can be developed (as opposed to just blindly throwing technology to the wall to see what sticks).

In addition to developing and testing the CYNETS simulation we were provided an additional unique opportunity to have access to IST students participating in a regional cyber security exercise. This access allowed us to interview students especially as to how they plan to attack a cyber threat situation (again both individually and in teams) and allowed a different kind of exploration as to how students identified, defined, investigated, and solved problems (or not) but from an alternative mode of understanding in contrast to an experimental design and simulation-based study. It is important because; (1) it was deemed state of the art for student teams (circa 2015), (2) it was provided by governmental officials who are fully aware of the embedded issues and constraints and therein represented what would be indicative of wicked

problems in the literature (Churchman 1967), and (3) these students will very soon be practicing cyber analysts so it is important to see how they interpret the cyber word and see what their shortcomings are in terms of distributed cognition and cyber situation awareness as they represent the new generation who will be combating threats of the future.

Many of the contextual and human-centric elements of decision making came into play (e.g., how they setup teams and utilize expertise, how they planned and re-planned the problem (metacognitive actions), how they knew how far to go in terms of pursuing a given path of solution, how they make team decisions, etc.) really influence their overall awareness of who they are, how things work together, and how the emerging context restrains what they can do in a limited timeframe (time pressure). Like many complex problems uncertainty and reasoning about uncertainty will impact the directionality of interdependent problem elements and how they become aware of what a threat is – where it exists at – and whether it is current.

Our intent with the qualitative interviews of students was to apply a coding scheme relative to the interests we have outlaid in work for the last six years (i.e., mainly pursuing a distributed cognition worldview that emphases learning and the evolving transactions between agents (human or computational) and the environment). Once our encoding scheme was applied to interviews we were able to use it to engage development of an initial concept-map based descriptive model (basically focused on planning and how people tackle the problems resident in the exercise). Concept maps afford descriptive based cognitive models which can be flexibly used in different ways but mainly as lightweight knowledge representation typologies emanating from knowledge elicitation activity (Zaff et al. 1993). We will discuss more about this below in the future work section.

Our overall goal with the modeling part of the Living Lab Approach, however, is to generate what we refer to as a layered, declarative concept map. This models declarative (and to some extend strategic) knowledge resident in a novice or expert cyber analyst for a given challenge problem within a specified context. As such it employs both cognitivistic and contextualistic layers of understanding and thinking as a person or team evolves through solvation of the problem presented. Because the map is heterarchical and is entrenched within the concept-relation-concept syntax it is maximally flexible and not over constrained. The coding scheme and concept maps of interviews of novice-level students can be useful to contrast and compare against expert concept maps for further elucidation, and inspire specific requirements for training.

In summary, much has been discovered. However, still more needs to be discovered about distributed cognition, information fusion, and teamwork as it contributes to establishing situation awareness in cyber defense. The approach taken here has always been to keep cycling to various components of the Living Lab as opportunity presents itself with eventually the intent to intervene in real world practice with; (a) effective cognitive technologies that truly impact positive use or (b) Innovative training for individuals and teams involved in complex cyber security problems. We turn now to discuss potential future work that directly follows directly from our research activities from this last year.

Future work. If one steps back from what has been accomplished, it clearly sets up some new research channels and extensions that could come into effect. We will briefly discuss what needs to be done in the next phase to further establish this line of research.

First, for the experimental research we feel that the next step is a full-scale experimental study involving CYNETS. Our hope would be to run an experimental design wherein hard fusion is crossed with soft fusion access. In this case soft fusion represents specific intelligence gathered on the threat that emerges during the course of the scenario. This would complement the hard fusion component and provide an additional dynamic in the teamwork component. This would provide a fuller scale test and actual experimental evaluation for publishing (assuming significant effects were obtained). The orchestration of the soft fusion element could be information provided only to one team member at a given point in time (simple soft data fusion) or unique information could be given to all three team members at different points in time (complex soft data fusion). There is experimental evidence that suggests team members only share that which is unique, which if true really limits the collective induction possibilities in the cyber context. Our intent would be to try to utilize ROTC students (as a kind of more DoD-aware student base) and compare with IST/SRA students (who are probably more aware of the technology and security-risk aspects of cyber systems).

Second, the coding schema data can be further propagated as a more integral concept map that involves layered representation to couple together different perspectives on knowledge that underlies situation awareness and distributed cognitive process. The first step would be to produce additional declarative, procedural, and strategic knowledge-based concept maps according to the planned overlay concept mapping typology (see Fig. 4). In the tradition of the AKADAM techniques (see Zaff et al. 1993) it is the intent to use the lightweight concept map model as the basis for; (1) establishing user needs and (2) defining new interface or cognitive technologies to obtain what Perkins (1986) refers to as 'knowledge as design'. The trajectory would be to use the entirely propagated layered concept map across every element as a basis for prototyping new designs that improve situation awareness in individual and distributed cognitive activities.

Third, the results from the experiment can be merged with the qualitative study to mutually inform each facet of our research (e.g., the research independent variables can be directly derived from qualitative data, and likewise the results of experiments can inform better cognitive models of individual cyber analysts and teams of analysts as they engage situation awareness in this kind of context.

Finally, another future goal would be to expound on descriptive lightweight models and create new middleweight models in the form of abstraction hierarchies and the cognitive decision ladder (Rasmussen et al. 1994). These models emphasize both structure and function more than concept maps but are given to make extant the actual contextual variants as well as providing representation of insights when learning proceeds. This is important because both kinds of models set up the cognitive systems engineering of adaptive resiliency systems of awareness in cyber operations which is needed where evolutionary uncertain information fusion foments across a highly distributed environment. Eventually, the goal would be to learn from the discoveries inherent in student exercises as well as the experimental designs in a way that really

strengthens and reinforces the cognitive models and ensuing technologies that are waiting to be developed for the next generation.

References

Bransford, J.D., Brown, A.L., Cocking, R.R.: How People Learn: Brain, Mind, Experience, and School. National Academy Press, Washington, DC (1999)

Brown, J.S., Collins, A., Duguid, P.: Situated cognition and the culture of learning. Educ. Res. **18** (1), 32–42 (1989)

Churchman, C.W.: Wicked problems. Manage. Sci. **14**(4), B141–B142 (1967)

Cooke, N.J., Gorman, J.C., Myers, C.W., Duran, J.L.: Interactive team cognition. Cogn. Sci. **37** (2), 255–285 (2013)

Descartes, R. (1664). L'Homme (treatise of man). Facsimile of the original French, together with an English translation by Hall, T.S.: Harvard University Press, Cambridge (1972). An abridged translation, by Stoothoff, R. is also available in Cottingham, J., Stoothoff, R., Murdoch, D. (Trans. & eds.) The philosophical writings of Descartes, vol. 1. Cambridge University Press, Cambridge (1985)

Ellis, A.P.J.: System breakdown: the role of shared mental models and transactive memory in the relationship between acute stress and tem performance. Acad. Manag. J. **49**, 576–589 (2006)

Endsley, M.R.: Toward a theory of situation awareness in dynamic systems. Hum. Factors J. Hum. Factors Ergon. Soc. **37**(1), 32 (1995)

Giacobe, N.A.: Application of the JDL data fusion process model for cyber security, in Multisensor. In: Braun, J. (ed.) Proceedings of the SPIE Multisource Information Fusion: Architectures, Algorithms and Applications, vol. 7710 (2010)

Giacobe, N.A.: A picture is worth a thousand alerts. In: Proceedings of the 57th Annual Meeting of the Human Factors and Ergonomics Society, San Francisco, CA, pp. 172–176 (2013)

Giacobe, N., Hall, D.-L.: Research opportunities and challenges for cyber systems risk management, 30 June 2015, 27 p., technical report for Penn State Applied Research Laboratory (2015)

Gibson, J.J.: The Ecological Approach to Visual Perception. Houghton Mifflin Company, Boston (1979)

Greeno, J.G.: Gibson's affordances. Psychol. Rev. **101**(2), 336–342 (1994)

Hart, S., Staveland, L.: Development of NASA-TLX (Task Load Index): Results of empirical and theoretical research. In: Hancock, P., Meshkati, N. (eds.) Human Mental Workload, vol. 52, pp. 139–183. North-Holland (1988)

Hayes-Roth, B., Hayes-Roth, F.: A Cognitive model of planning. Cogn. Sci. **3**, 275–310 (1979)

Hoffman, R.R., Nead, J.M.: General contextualism, ecological science and cognitive research. J. Mind Behav. **4**(4), 507–559 (1983)

Hutchins, E.: Cognition in the Wild. MIT Press, Cambridge (1995)

James, W.: The Principles of Psychology. Harvard University Press, Cambridge (1981). Originally published in 1890

Klein, G.: Sources of Power: How People Make Decisions. MIT Press, Cambridge, MA (1999)

Klein, G., Ross, K.G., Moon, B.M., Klein, D.E., Hoffman, R.R., Hollnagel, E.: Macrocognition. IEEE Intell. Syst. **18**(3), 81–85 (2003)

Laughlin, P.: Collective induction: Twelve postulates. Organ. Behav. Hum. Decis. Process. **80**(1), 50–69 (1999)

Lewis, K.: Knowledge and performance in knowledge-worker teams: a longitudinal study of transactive memory systems. Manage. Sci. **50**(11), 1519–1533 (2004)

Mace, W.M.: James J. Gibson's strategy for perceiving: Ask not what's inside your head, but what your head's inside of. In: Shaw, R.E., Bransford, J. (eds.) Perceiving, Acting, and Knowing. Erlbaum, Hillsdale (1977)

Matthew, M.D., Beal, S.A.: Assessing situation awareness in field training exercises. US Army Research Institute for the Behavioral and Social Sciences (2002)

McNeese, M.D.: Humane intelligence: a human factors perspective for developing intelligent cockpits. IEEE Aerosp. Electron. Syst. **1**(9), 6–12 (1986)

McNeese, M.D.: An ecological perspective applied to multi-operator systems. In: Brown, O., Hendrick, H.L. (eds.) Human Factors in Organizational Design and Management - VI, pp. 365–370. Elsevier, The Netherlands (1996)

McNeese, M.D., Cooke, N.J., Champion, M.: Situating cyber-situational awareness. In: Proceedings of the 10th International Conference on Naturalistic Decision Making (NDM 2011), 31 May–3 June, Orlando, FL (2011)

McNeese, M.D., Mancuso, V.F., McNeese, N.J., Glantz, E.: What went wrong? What can go right? A prospectus on human factors practice. In: Proceedings of the 6th International Conference on Applied Human Factors and Ergonomics (AHFE 2015) and the Affiliated Conferences, AHFE, Las Vegas, NV, July 2015

McNeese, M.D., Pfaff, M., Connors, E.S., Obieta, J., Terrell, I., Friedenberg, M.: Multiple vantage points of the common operational picture: Supporting complex teamwork. In: Proceedings of the 50th Annual Meeting of the Human Factors and Ergonomics Society, San Francisco, CA, pp. 26–30 (2006)

McNeese, M.D., Vidulich, M. (eds.): Cognitive systems engineering in military aviation environments: Avoiding cogminutia fragmentosa. Wright-Patterson Air Force Base, OH: Human Systems Information Analysis Center (HSIAC) (2002)

Moreland, R.L., Myaskovsky, L.: Exploring the performance benefits of group training: Transactive memory or improved communication? Organ. Behav. Hum. Decis. Process. **82**(1), 117–133 (2000)

Newell, A., Shaw, J.C., Simon, H.A.: Elements of a theory of human problem solving. Psychol. Rev. **23**, 342–343 (1958)

Newell, A., Simon, H.: Human Problem Solving. Prentice-Hall, Englewood Cliffs (1972)

Pearsall, M.J., Ellis, A.P.J.: The effects of critical team member assertiveness on team performance and satisfaction. J. Manag. **32**, 575–594 (2006)

Perkins, D.N.: Knowledge as Design. Erlbaum, Hillsdale (1986)

Rasmussen, J., Pejtersen, A.M., Goodstein, L.P.: Cognitive Systems Engineering. Wiley, New York (1994)

Reifers, A.: Network access control list situation awareness. (Unpublished doctoral dissertation). The Pennsylvania State University. University Park, PA (2010)

Rimland, J., Ballora, M.: Using complex event processing (CEP) and vocal synthesis techniques to improve comprehension of sonified human-centric data. In: SPIE Proceedings, vol. 9122. Next-Generation Analyst II, 22 May 2014

Salas, E., Fiore, S.M., Letsky, M.: Theories of Team Cognition: Cross-Disciplinary Perspectives. Routledge, New York (2012)

Scielzo, S., Strater, L.D., Tinsley, M.L., Ungvarsky, D.M., Endsley, M.R.: Developing a subjective shared situation awareness inventory for teams. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 53, p. 289 (2009)

Shiravi, H., Shiravi, A., Ghorbani, A.: A survey of visualization systems for network security. IEEE Trans. Vis. Comput. Graph. **18**(99), 1 (2011)

Stall, D., Yu, T., Crouser, R. J., Damodaran, S., Nam, K., O'Gwynn, D., McKenna, S., Harrison, L.: Visualization evaluation for cyber security: trends and future direction. In: Proceedings of the Eleventh Workshop of Visualization for Cyber Security, pp. 49–56 (2014)

Stasser, G., Titus, W.: Pooling of unshared information in group decision making: Biased information sampling during discussion. J. Pers. Soc. Psychol. **48**, 48–1467 (1985)

Taylor, R.M.: Situational awareness rating technique (SART): The development of a tool for aircrew systems design. Situational awareness in aerospace operations, AGARD-CP- 478. Neuilly Sur Seine, France: NATO-AGARD, 3/1-3/17 (1990)

Tyworth, M., Giacobe, N., Mancuso, V., McNeese, M., Hall, D.: A human-in-the-loop approach to understanding situation awareness in cyber defense analysis. EAI Endorsed Trans. Secur. Saf. **13**(2), 1–10 (2013)

Young, M., McNeese, M.: A situated cognition approach to problem solving. In: Hancock, P., Flach, J., Caid, J., Vicente, K. (eds.) Local Applications of the Ecological Approach to Human Machine Systems, pp. 359–391. Erlbaum, Hillsdale (1995)

Wegner, D.M.: Transactive memory: a contemporary analysis of the group mind. In: Mullen, B., Goethals, G.R. (eds.) Theories of Group Behavior, pp. 185–205. Springer, New York (1986)

Wilson, M.: Six views of embodied cognition. Psychon. Bull. Rev. **9**, 625–636 (2002)

Zaff, B.S., McNeese, M.D., Snyder, D.E.: Capturing multiple perspectives: a user-centered approach to knowledge acquisition. Knowl. Acquisition **5**(1), 79–116 (1993)