REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
31-08-2012	Book	-

4. TITLE AND SUBTITLE
An Alternative Framework for Research on Situational Awareness in Computer Network Defense

5a. CONTRACT NUMBER
W911NF-09-1-0525

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611103

6. AUTHORS
McMillan, E., Tyworth, M.

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Pennsylvania State University
Office of Sponsored Programs
The Pennsylvania State University
University Park, PA 16802 -7000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
56161-CS-MUR.47

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
In this chapter we present a new framework for the study of situation awareness in computer network defense (cyber-SA). While immensely valuable, the research to date on cyber-SA has overemphasized an algorithmic level of analysis to the exclusion of the human actor. Since situation awareness, and therefore cyber-SA, is a human cognitive process and state, it is essential that future cyber-SA research account for the human-in-the-loop. To that end our framework presents a basis for examining cyber-SA at the cognitive, system, work, and enterprise levels of

15. SUBJECT TERMS
Situational Awareness, Computer Network Defense

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Peng Liu
UU	UU	UU	UU		19b. TELEPHONE NUMBER: 814-863-0641

Report Title

An Alternative Framework for Research on Situational Awareness in Computer Network Defense

ABSTRACT

In this chapter we present a new framework for the study of situation awareness in computer network defense (cyber-SA). While immensely valuable, the research to date on cyber-SA has overemphasized an algorithmic level of analysis to the exclusion of the human actor. Since situation awareness, and therefore cyber-SA, is a human cognitive process and state, it is essential that future cyber-SA research account for the human-in-the-loop. To that end our framework presents a basis for examining cyber-SA at the cognitive, system, work, and enterprise levels of analysis. In describing our framework we present examples of research that are emblematic of each type of analysis.

An Alternative Framework for Research on Situational Awareness in Computer Network Defense

Eric McMillan
College of Information Sciences & Technology
The Pennsylvania State University, United States

Michael Tyworth
College of Information Sciences & Technology
The Pennsylvania State University, United States

ABSTRACT

In this chapter we present a new framework for the study of situation awareness in computer network defense (cyber-SA). While immensely valuable, the research to date on cyber-SA has overemphasized an algorithmic level of analysis to the exclusion of the human actor. Since situation awareness, and therefore cyber-SA, is a *human* cognitive process and state, it is essential that future cyber-SA research account for the human-in-the-loop. To that end our framework presents a basis for examining cyber-SA at the cognitive, system, work, and enterprise levels of analysis. In describing our framework we present examples of research that are emblematic of each type of analysis.

INTRODUCTION

In this chapter we propose a theoretical framework of cyber situation awareness (cyber-SA) that attempts to capture cyber-SA as both a process and a state that involves knowledge, action, and the environment. In terms of computer network defense cyber-SA, and situation awareness more broadly, has been generally understood to be the ability to perceive, understand, and project the future status of elements in the environment (Endsley, M. R., 2000). Relying on this definition of cyber-SA, research has been conducted in several contexts over the last twenty-five years, including the military, aviation, air

traffic control, and command, control, communication and intelligence (C4i) environments (Salmon, P., Stanton, N., Walker, G., & Green, D., 2006). Despite the proliferation of research in these areas, minimal research has been conducted on SA as it is developed in computer network defense. This is problematic because much of the research on traditional SA may not be as applicable to the highly dynamic and complex environment of computer network defense (Barford, P. et al., 2010; Tadda, G., Salerno, J. J., Boulware, D., Hinman, M., & Gorton, S., 2006; Yen, J. et al., 2010). For example, with cyber-SA there is a greater separation between the user and the physical system due to the inherent virtuality of the environment and this separation presents domain-specific challenges.

Drawing on an alternative theory of SA as both process and state, we argue that the proposed framework should guide research into the study of the internal cognitive processes an analyst employs to make sense of data and information; and how those processes are facilitated by the interfaces and tools analysts employ. Our proposed framework is distinguished from other approaches to understanding cyber-SA in that it moves beyond the artifact and individual cognition and accounts for work-, team-, and enterprise-level factors that impact cyber-SA.

THEORETICAL BACKGROUND

A review of the extant literature reveals that the prior work on situation awareness draws primarily from the work done by Micah Endsley (1995). Endsley theorized SA as consisting of three levels. Level 1 SA represents the perception of cues in the environment salient to the individual's task at hand. Note here, that it is only the perception of cues salient to the task at hand that matters in terms of Level 1 SA. Indeed perception of non-salient cues, or noise, can be understood to degrade SA. Level 2 SA is the comprehension of the perceived cues to include comparison against memory, orientation, and prioritization. Level 3 SA is the projection of future states based on the individual's comprehension. At all three levels temporality and space play a critical role. Consider the operation of a motor vehicle in traffic. Perceiving that a traffic signal is yellow (Level 1), the operator comprehends that the signal is in a

state of change and projects that the light will soon change again to red which means to stop (Level 2) and so he should begin decelerating (Level 3).

The three levels of situation awareness are generally understood to be hierarchical, and implicitly sequential, in nature. That is comprehension is dependent on perception, and projection is dependent on comprehension. Failure to perceive salient cues leads to a lack of comprehension of the current environmental state and an inability to accurately project the future state of the environment. An individual may fail to achieve Level 1 SA or Level 2 SA and still correctly project the future state of the environment through random chance. At the same time, an individual may have perfect SA and still make errors due to insufficient resources (Endsley, M. R., 2000).

Ensdley's model of situational awareness is the most prominent of three models of SA that have been previously theorized in the literature. Two others include SA as a set of cognitive subsystems; and SA as an environmentally driven consciousness – referred to as the 'embedded-interactive' model (Stanton, N. A., Chambers, P. R. G., & Piggott, J., 2001). It is this latter approach that drives this research provides the foundation for our model cognitive process.

The embedded-interactive model of SA conceptualizes SA as spanning the intersection of the human actor and the environment (Smith, K. & Hancock, P. A., 1995). Similar to other socio-technical theory, in the embedded-interactive model SA is comprised of both internal cognitive processes and external context. In other words, situation awareness is both an internal cognitive process and cognitive state that is directly shaped by the environment in which the human actor resides. Drawing on knowledge about perceived cues from the environment, the human actor takes goal-based actions derived from knowledge and assesses the outcomes, and the assessment produces updates to knowledge.

Consider the following example. A network security analyst looking at network traffic logs becomes aware that the database server has received multiple failed authentication attempts from an IP address that normally does not communicate with the database server [*environment*]. Based on prior

experience, the analyst speculates that an intruder is attempting to gain unauthorized access to the server [*knowledge*] and as a result implements a new firewall rule that drops all traffic from the suspicious IP address to his network [*action*]. If the unauthorized attempts cease, the goal of preventing an intrusion into the database is realized and the analyst has situation awareness. If the attempts continue, the analyst does not have situation awareness because he has misunderstood the state of the environment; he adjusts his knowledge based on this new information, and takes additional actions.

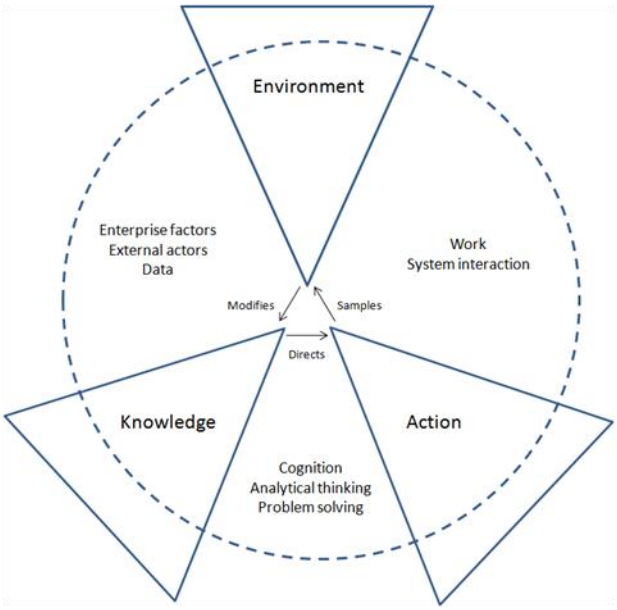

Figure 1 - Modified embedded-context model of SA

One of appeals of this theory of SA is that it speaks to how individuals develop "the big picture" of their environment, something that is a fundamental challenge in computer network defense. Understanding how a network analyst forms and maintains an overall understanding of the state of the computer network, the 'big picture,' and the role of situation awareness in those processes is one of the fundamental goals of cyber-SA research.

There is a second element of Smith & Hancock's theory of SA that may prove to be particularly useful to cyber-SA research and that is the concept of risk spaces. A risk space is a two-dimensional (but potentially n-dimensional) matrix of human performance (see Figures 2 and 3 below). The axes of the risk space represent those factors that negatively impact safety (or in the case of computer network

defense, the integrity of the network and associated assets). Objects are plotted on the matrix and based on their location and vector, one can determine their priority. Smith & Hancock (1995) demonstrated the concept using the rate of change in distance and lateral distance as their dimensions and plotted the likelihood of aircraft collisions in a specified airspace. In the computer network defense context, one might plot number of clients at risk of infection from a computer virus, and the speed of the virus' propagation to assess threats.

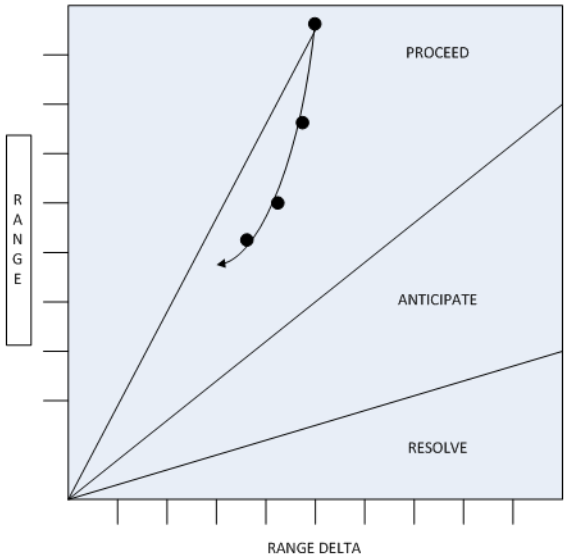

Figure 2 Smith & Hancock's Aviation Risk Space

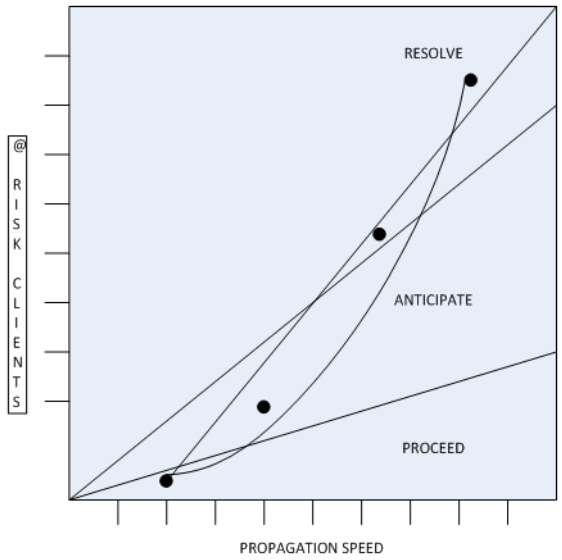

Figure 3 - A CND Risk Space

In the aviation example, the closer the distance and greater the rate of decrease in range between two aircraft the greater the likelihood of a collision. In the computer network defense example, the greater the number of clients at risk and the greater the propagation rate of the infection, the greater the likelihood of catastrophic consequences for the network. This method of assessing risk may prove a useful way for assessing cyber threats and determining courses of action thereby increasing the analyst's SA.

What is Cyber Situation Awareness?

Barford *et al.* (2010) list 7 dimensions of cyber-SA (see Table 1). These dimensions range from awareness of the current situation to awareness of plausible future outcomes. Of the seven dimensions

described, the extant research on cyber-SA has focused on dimensions one, six, and seven and largely relied upon the three-level model of SA as a conceptual foundation. Researchers have relied on the three levels of SA described in the three-level model – perception, comprehension, and projection – to both describe what cyber-SA facilitating tools should do (increase perception and comprehension of salient cues) and to assess the efficacy of such tools (e.g. – how well do tools improve projection accuracy and efficacy?). The alignment of the three-level model of SA with the JDL data fusion process model (Llinas, J. & Hall, D. L., 1998; Tadda, G., et al., 2006) is another reason for its utility in cyber-SA research given the centrality of data fusion to computer network defense. Though the three-level model has been the dominant model employed in cyber-SA research, there are three widely acknowledged differences between cyber-SA and standard SA.

1.	Awareness of current situation
2.	Awareness of impact of attack
3.	Awareness of evolution of situation
4.	Awareness of adversary behavior
5.	Awareness of situational cause
6.	Awareness of information quality and quality of derived decisions
7	Awareness of plausible future outcomes

Table 1 Dimensions of Cyber-SA

One difference between cyber-SA and standard SA is that the scope of the environment within which cyber-SA occurs is significantly larger than those in which SA has previously been studied such as flying a fighter jet or driving a car. The amount of information generated in real time by sensors monitoring cyberspace – including other human actors, system logs, intrusion detection systems, etc. – can easily overwhelm the human analyst making it virtually impossible to perceive the salient cues from the environmental noise (Barford, P., et al., 2010; Tadda, G., et al., 2006; Tadda, G. P. & Salerno, J. S., 2010; Yang, S. J., Byers, S., Holsopple, J., Argauer, B., & Fava, D., 2008). The analyst involved in computer network defense must not only process information about attacks on their system (identity and

motivation of the attacker, intended outcome of attack, target of attack, likely outcome(s) of the attack) but must also continually evaluate the state of their network (priority, vulnerabilities, current status, etc.). As a result, reducing the cognitive load computer network defense imposes on the human analyst has been the focus on much of the cyber-SA research (c.f., Barford, P., et al., 2010; Bass, T., 2000; Gregoire, M. & Beaudoin, L., 2005; Yen, J., et al., 2010).

A second distinction between cyber-SA and 'standard' SA is the amount of contextual information against which cues can be evaluated. A person driving a car does so in a relatively constrained environment. Contextual cues are omnipresent (the light is red, the road is wet, the other cars are all stopped, etc.). This represents a very different reality from that of the network analyst for which the contextual cues are incomplete and uncertain (Yen, J., et al., 2010). Lack of context can make determining an attacker's intent and capabilities very difficult if not impossible. For example, a system can come under attack but not be the intended target as in the case of the Stuxnet worm which infected multiple systems but had a single (at the time) undetermined target (Clayton, M., 2010). Similarly, awareness of an attacker's intent may be limited to the intended exploit or the targeted system instead of awareness of the attacker's broader goal of attacking a particular system in a particular manner. For example, even though security experts understand how the Conficker worm works, it is unclear who the attackers are and what they are attempting to achieve (Bowden, M., 2010). Lack of contextual information makes it difficult for analysts to project the appropriate course of action.

The third distinction between cyber-SA and standard SA is the speed at which the environment evolves. Cyberspace is a hyper-dynamic environment in which the environmental state is continually evolving. Humans are incapable of cognitively keeping pace with the rate of change in cyberspace Network analysts can become easily overwhelmed in such an environment and rarely form complete mental models impacting their decision-making processes and the available courses of action (Gregoire, M. & Beaudoin, L., 2005; Yang, S. J., et al., 2008). A rapidly changing information environment requires that analysts be able to identify salient new information and process it against existing knowledge. As a

result, the performance speed of SA systems is much higher than that of physical systems (Barford, P., et al., 2010).

A review of the cyber-SA literature reveals that most cyber-SA research has adopted a tool or algorithmic perspective of cyber-SA (Orlikowski, W. J. & Iacono, C. S., 2001); that is, the research has focused primarily on the development of complex computer programs employing probabilistic models to improve cyber-SA. Examples of this research stream include examining how information visualizations can enhance cyber-SA (D'Amico, A. & Kocka, M., 2005; Gregoire, M. & Beaudoin, L., 2005) the development of frameworks for evaluating cyber attacks (Mathew, S., Shah, C., & Upadhyaya, S., 2005; Sudit, M., Stotz, A., Holender, M., Tagliaferri, W., & Canarelli, K., 2006); and the use of complex programs to project intrusion activity and assess the impacts of cyber attacks (Shen, D., Chen, G., Haynes, L., & Blasch, E., 2007; Yang, S. J., et al., 2008). Two notable exceptions are D'Amico et al.'s (2005) cognitive task analysis of information assurance analysts and Yen et al.'s (2010) development of a hypothesis-reasoning framework using a recognition-primed decision model. While this is important and impactful work, the emphasis on computation and the development of IT artifacts in Cyber-SA research has limited the degree to which the factors that impact cyber-SA and the processes by which cyber-SA is developed and maintained are understood because the human element has largely been omitted from Cyber-SA research.

We argue that the human agent is the most important element in computer network defense and therefore a more holistic approach to Cyber-SA research will contribute to a more thorough understanding of Cyber-SA that is grounded in professional practice. To this end, we propose a new model of cyber-SA that accounts for both human and machine actors as well as enterprise-level factors that can influence cyber-SA.

AN ALTERNATIVE FRAMEWORK FOR CYBER-SA

We propose an alternative framework for cyber-SA for three reasons. One, while the prior work on cyber-SA has been both informative and important, it has focused almost exclusively on developing new technological artifacts to the exclusion of the human actor in computer network defense. As a result, our understanding of cyber-SA has grown but remains incomplete. Through this framework we seek to reintroduce the human element into the human-computer loop.

Two, we argue that to understand how the human analyst makes sense of the cyber-environment in computer network defense, it is critical to understand the broader work context within which cyber-SA is developed. In the literature cyber-SA is understood to be unique because of the uniqueness of the environment within which it is developed. Yet little attention has been paid to the ways in which the cyber environment is actually different from other work contexts. In order to understand the unique cognitive demands presented by cyber environment we must seek to understand how analysts engaged in computer network defense actually work.

Three, we seek to extend theory of situation awareness by focusing attention on intersection of the human agent and the environment. The cyber environment plays a critical role in cyber-SA. The reliance on the three-level model of SA in cyber-SA research implicitly treats SA as a cognitive state. Yet the dynamism of the cyber environment suggests that we may be better served conceptualizing cyber-SA as a process rather than a state.

The framework

We frame cyber-SA as a domain-specific instance of Smith & Hancock's (1995) model of situation awareness. In this conceptualization, SA is comprised of three dimensions: the environment (or real world), knowledge (or the human's internal cognitive state), and action (interaction with the environment). Each individual dimension is comprised of elements that impact cyber-SA.

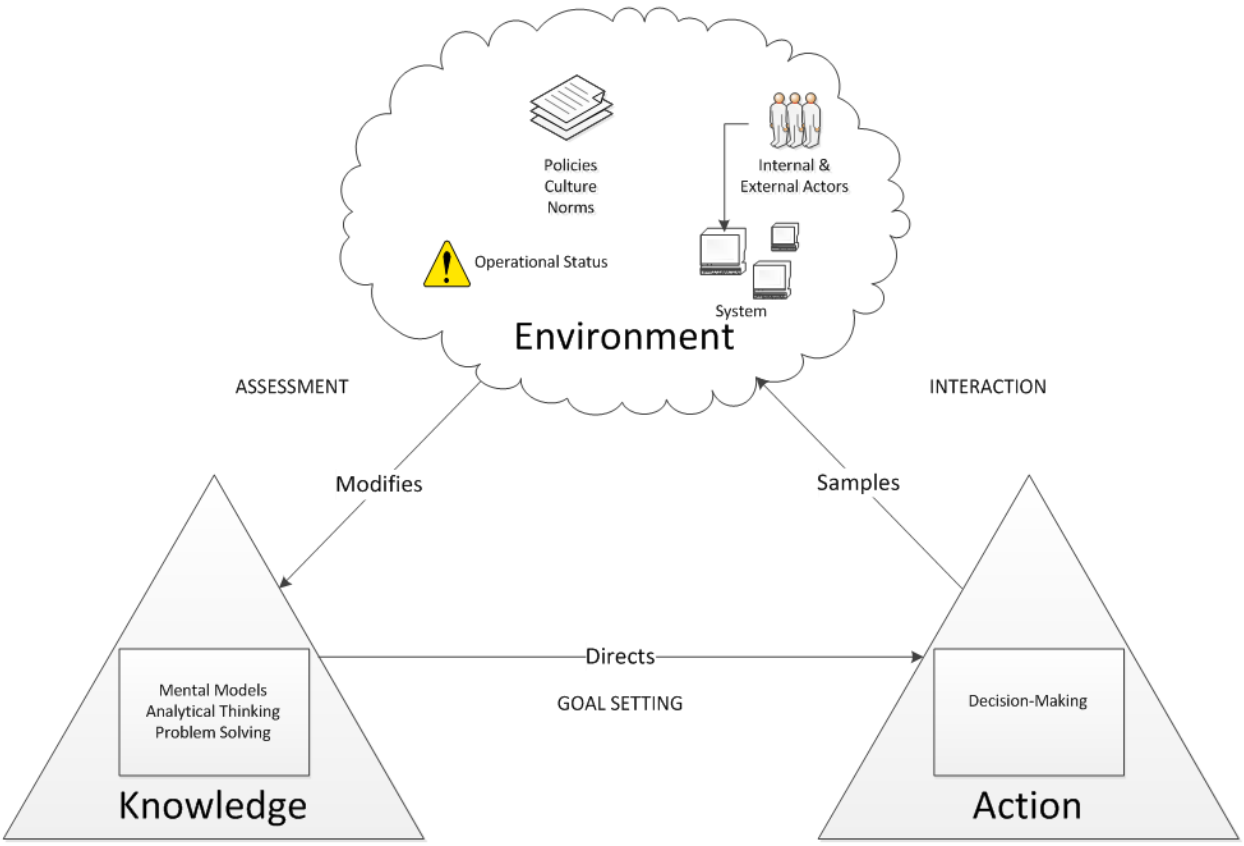

Figure 4 - Model of Cyber-SA as a Process

Interaction between human actor and the network occurs on the axis linking action and the environment. Assessment of the action's impact on the environment takes place along the axis between the environment and knowledge. Goal setting occurs after the environment has been assessed and the actor's knowledge updated and informs the next action to be taken.

For example, within the *knowledge* dimension we find human cognitive processes such as memory, attention, analytical thinking and problem solving, and mental models. This dimension represents the internal processes and structures by which the analyst draws conclusions about the current state of the environment and informs the setting of task goals (e.g., close a port via firewall rule to prevent unauthorized access). The *action* dimension is where the ends of the human-machine loop connect. Decision-making strategies and processes play a key role in the *action* dimension as it at this point in the SA process that a human determines how to interact with the environment to achieve SA.

Environment

Within the *environment* dimension we find elements such as network operational status (operational, strategic, or critical), enterprise factors such as organizational norms and policies, the computer network system and associated interfaces, and actors both internal and external to the organization. This list is not exhaustive and more elements are likely to emerge via empirical field-based research. Together these elements comprise the real-world environment within which the network analyst operates. For the purposes of this discussion we will focus on the enterprise factors and system-level issues.

Cyber-SA in the Enterprise

Analysts engaged in computer network defense predominantly do so in an organizational context (public, private, and military), and this context can play a critical role in the analyst's ability to develop and maintain Cyber-SA. Here we are attempting to capture the mediating influence of organizational policies, mode, and culture on the analyst's Cyber-SA. An analyst working in an organization operating in crisis mode is likely to be attending to different environmental cues and have access to different informational resources than analyst working in an organization in normal operating mode. Similarly, an analyst working in an organization that has a permissive culture in regards to employee use of IT faces different challenges in understanding the current state of the internal cyberspace than one who works in an organization that more tightly controls its IT infrastructure.

Prior research supports the inclusion of enterprise-level factors in the framework. Chang and Lin (2007) found a significant correlation between organizational culture and information security management (ISM). Specifically, the ISM principle of confidentiality was negatively correlated with a cultural of cooperation; while an organizational culture of effective and

consistency were positively associated with the ISM principles of integrity, availability and accountability. Conversely, organizational cultural traits associated with flexibility were found to not be associated with ISM principles. The authors suggest that a flexible organizational culture is likely to run counter to effective information security management. Based on these findings, from cyber-SA perspective we should expect Cyber-SA is more difficult to develop and maintain in an organization with a flexible culture than one with a control-oriented culture.

Similarly, organizational factors may serve to limit the network security analyst's ability to be cognizant of vulnerabilities in their cyber environment. In a study of computer information security professionals Kraemer, Carayon, & Clem (2009) identified nine organizational areas that can result in vulnerabilities in the computer network defense system. These areas include lack of access to critical computer network defense information, too much policy, an absence or lack of policy documentation, inadequate training, and overburdened security resources. It is easy to how these factors can serve to limit the Cyber-SA of the analyst responsible for maintaining his organization's computer network defense. For example, if the analyst's workload is too high, the amount of attention the analyst can dedicate to any single item is limited, therefore increasing the likelihood that the analyst will miss (fail to perceive) some critical environmental cue.

Understanding how enterprise-level moderators influence cyber-SA is a critical step towards the goal of developing technological tools and work practices that facilitate the development and maintenance of cyber-SA by computer network defense professionals. Indeed, as is typical in other work domains (Norman, D. A., 1990), failure to account for the enterprise context in which computer network defense occurs is likely to result in the production of tools of limited utility to the professional practitioner.

Cyber-SA and the System

Cyber-SA research on system-level issues deal with the development and design of the technological tools a human analyst uses in computer network defense. One of the challenges of developing SA in the cyber environment is the human actor is decoupled from the physical environment (Stanton, N. A., et al., 2001). Indeed, unlike an automobile or fighter jet, there is no physical environment for the analyst to use senses other than sight to gauge the status of the environment. Everything the computer network defender knows about the state of her network is limited to the feedback displayed on screen (Norman, D. A., 1990). The more automated the computer network defense system is, the more physically- and mentally isolated from the system the analyst becomes (Norman, D. A., 1990). This reality presents numerous challenges to practitioners and designers alike.

One challenge is presenting information in manner that is informative to the analyst. Cues that are too subtle get overlooked. Too many cues overload and distract the analyst. Cues that are too simplistic do not convey enough information to be meaningful and thus useful. Examples of system breakdowns resulting inappropriate or incomplete feedback are manifest and include, the Three Mile Island accident and the crash of American Airlines Flight 191 (Perrow, C., 1999).

As noted previously, the majority of the scholarly work on cyber-SA has been on what we identify as system-level issues. Much of the work has been oriented towards developing better methods of data fusion to improve cyber-SA (c.f., Bass, T., 2000; Mathew, S., et al., 2005; Sudit, M., Stotz, A., & Holender, M., 2005; Sudit, M., et al., 2006). Others have focused on developing methods or tools for projecting intrusion activity and assessing the impact of cyber-attacks (c.f., Shen, D., et al., 2007; Yang, S. J., et al., 2008; Yen, J., et al., 2010). Finally, there is an increasing amount of work being done on developing visualizations of network security data to enhance cyber-SA (c.f., D'Amico, A. & Kocka, M., 2005; D'Amico, A., et al., 2005; Gregoire, M. & Beaudoin, L., 2005). It is likely that much of the work on cyber-SA will continue to be system-level research. The work being done on developing methods for

visualizing network data seem particularly promising in terms of reducing the mental-isolation of the human operator engaged in computer network defense.

Knowledge

The second core dimension of our framework represents the knowledge of the human actor about the state of the cyberspace. The knowledge dimension consists of the fundamental cognitive processes that have been associated with situational awareness such as the aforementioned perception, comprehension, and projection, other cognitive constructs such as mental models, and analytical thinking techniques such as structured analysis and problem solving. In this chapter we focus on the last element – analytical and problem-solving techniques.

The similarity of computer network defense to intelligence analysis

For the human operator, the process of defending a computer network from attack similar to that of an intelligence analyst attempting to make sense of a geopolitical situation. Intelligence analysis involves ascertaining meaning through the development of hypotheses and estimates, assessing those hypotheses and estimates, and drawing conclusions about the correct course of action in the future based on the assessments (Clark, R. M., 1996). Like the intelligence analyst, the cyber-security analyst is also forms hypotheses and estimates about the nature of attacks on his network, assesses those hypotheses, and makes decisions about how to proceed based on those assessments. Cyber security analysis and intelligence analysis are similar as well in terms of the errors analysts commonly experience. Most major failures in intelligence analysis take the form of incorrect or incomplete analysis or failure to take the correct action based on the analysis (Clark, R. M., 1996), and we see this with cyber-security analysts as well (Yen, J., et al., 2010). Given the similarities of the two domains, we are likely to find utility in the tools and processes that have developed out of research on intelligence analysts. We find the research on structured analysis to be particularly promising.

Structured Analysis

Structured analysis, or structured problem solving, is an approach to analysis intended to overcome obstacles to analytical thinking such as bias, satisficing, and extrapolation (Jones, M. D., 1995). There are multiple structured analytical techniques ranging from the relatively simple such as a pro/con analysis to the complex such as the utility matrix and advanced utility analysis techniques (see Table 2).

Problem Restatement
Pros/Cons and Fixes
Divergent/Convergent Thinking
Sorting, chronologies & timelines
Casual flow diagramming
Matrices
Decision/event tree
Weighted ranking
Hypothesis testing
Devil's advocacy
Probability tree
Utility matrix
Advanced utility analysis

Table 2 Structured Analysis Techniques

There is a significant opportunity to incorporate prior work on structured analysis into research on cyber-SA for computer network defense. For example, what impact does the use of structured analysis impact human cyber-SA? How can structured analytical techniques be automated to improve both system and human cyber-SA? How do analytical coping strategies such as extrapolation (Folker Jr., R. D., 2000) serve to impede the development of cyber-SA?

Indeed, much of the algorithmic work on cyber-SA has implicitly incorporated structured analysis techniques. For example, Yen *et al.*'s (2010) work seeks to improve cyber-SA through the use of intelligent agents engaging in hypothesis testing. Research on the development of attack graphs to improve cyber-SA employs Bayesian networks are similar to probability trees (Li, J., Ou, X., & Rajagopalan, R., 2010). D'Amico *et al.*'s (2005) model of threat assessment is, in essence, a

decision/event tree. These examples demonstrate that structured analytical techniques are central to cyber-SA research. In addition to continuing this important work, we advocate for research on the application of structured analysis techniques to include the human operator.

Action

The action dimension of our framework reflects the goals and actions an individual takes to interact with the cyberspace environment based on his understanding of the situation. In the theory underlying our proposed framework, the degree of cyber-SA is measured by the degree to which the individual's chosen action is the correct action in response to environmental cues. When the action is correct, the individual has cyber-SA; when the action is incorrect the analyst does not have cyber-SA.

In computer network defense terminology action could mean responding to an attack, detecting and identifying threats, identifying and addressing vulnerabilities, forensic analysis, and other activities. In many ways, cyber-security actions mimic the OSI network model with actions occurring at different layers – such as the network layer or application layer.

Cyber Security Elements	Description
Information Security	Protection of information assets from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction (Allen, J. H., 2001)
Application Security	Measures taken throughout an applications' lifecycle to prevent exceptions in the application's security policy or its underlying system through flaws in design, development, deployment or maintenance.
Operating System Security	Measures taken through an operating system's lifecycle to prevent exceptions to the operating system's security policy.
Network Security	The provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of service to the network or network-accessible resources.
Physical Security	Physical measures to secure the information resources.

Table 3 Multilayer approach to cyber-security adapted from (Lan, L.-n., Liu, X.-y., & Yang, T.-h., 2009)

The action component of cyber-SA is perhaps the least researched and most poorly understood aspect of cyber-SA. Some work has been done on action as a component of cyber-SA already. Examples of this work include D'Amico's *et al.*'s (2005) cognitive task analysis investigating how cyber-security analysts form goals, make decisions, and engage in work. Though applied to the assessment of attack threat vectors, the measures proposed by Tadda and Salerno (2010) may also prove useful in assessing the quality of action taken by the human analyst. Other outstanding questions related to action that need to be addressed include: how do analysts choose a specific course of action? What role does experience play in an analysts' ability to correctly choose a course of action? What triage strategy to analysts employ when prioritizing what goals to act on?

FUTURE RESEARCH DIRECTIONS

One of the benefits of the framework proposed in this chapter is its applicability to multiple levels of analysis. The knowledge dimension of the model describes internal cognitive processes and structures. The action component describes the interaction of the actor with the environment. The environment dimension accounts for system, enterprise, and operational factors. In accounting for cyber-SA at these different levels we will develop better knowledge of how cyber-SA is achieved and maintained in practice, while at the same time capitalizing and extending the important scholarly work that has been done in the domain of computer network defense and situation awareness.

This chapter presents a basis for future research in two key directions: the extension and elaboration of extant situation awareness theory; and the expansion of cyber-SA research beyond an algorithmic level of analysis towards a more holistic view. Endsley's (1995) three-level model has proven useful and instructive in cyber-SA research, particularly as cyber-SA relates to information fusion; but there remain many unanswered questions about cyber-SA that the three-level model may not be adequate to answering. In particular, that the three-level model of SA treats SA as a state rather than a process suggests that it is ill-suited to application in as dynamic and complex an environment as cyberspace.

In describing our framework we have sought to identify exemplar research that is representative of the concepts we are describing. The examples we have cited are by no means exhaustive. There remains much work to be done, particularly in regards to developing empirical knowledge of how cyber-security professionals actually work. We encourage cyber-SA scholars to take up this challenge along with us so that we may all benefit from a better understanding of cyber-SA as it relates to computer network defense.

CONCLUSION

In this chapter we have argued for an alternative, more contextually-grounded framework of cyber-situational awareness that more thoroughly accounts for the interaction of the human agent with the complex cyberspace environment. Our hope is that this framework will serve as a starting point for developing a more thorough knowledge of situation awareness as a cognitive state and process, cyber-security as a practice, and the ways in which information technologies can be designed and enhanced to improve the defenders of computer networks ability to understand the big picture of their cyberspace.

REFERENCES

Allen, J. H. (2001). *The CERT Guide to System and Network Security Practices*. Redwood City, CA: Addison-Wesley.

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, J., Griffin, S., Jajodia, S., et al. (2010). Cyber SA: Situational Awareness for Cyber Defense - Issues and Research. In S. Jajodia, P. Liu, V. Swarup & C. Wang (Eds.), *Cyber Situational Awareness* (pp. 3-14). New York: Springer.

Bass, T. (2000). Intrusion detection systems and multisensor data fusion. *Communications of the ACM, 43*(4), 99-105.

Bowden, M. (2010). The Enemy Within. *The Atlantic Monthly*. Retrieved from http://www.theatlantic.com/magazine/archive/2010/06/the-enemy-within/8098/

Chang, S. E., & Lin, C. S. (2007). Exploring organizational culture for information security management. *Industrial Management + Data Systems, 107*(3), 438-458.

Clark, R. M. (1996). *Intelligence Analysis: Estimation and Prediction*. Baltimore: American Literary Press.

Clayton, M. (2010). Stuxnet malware is 'weapon' out to destroy...Iran's Bushehr nuclear plant? *Christian Science Monitor*. Retrieved from http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant

D'Amico, A., & Kocka, M. (2005, October 26). *Information assurance visualizations for specific stages of situational awareness and intended uses: lessons learned.* Paper presented at the IEEE Workshop on Visualization for Computer Security (VizSEC 05), Minneapolis, Minnesota.

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005, September 26-30). *Achieving Cyber Defense Situational Awareness: A Cognitive Task Analysis of Information Assurance Analysts.* Paper presented at the Human Factors and Ergonomics Society 49th Annual Meeting, Orlando, FL.

Endsley, M. R. (1995). Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 37*(1), 32-64.

Endsley, M. R. (2000). Theoretical Underpinnings of Situationa Awareness: A Critical Review. In M. R. Endsley & D. J. Garland (Eds.), *Situation Awareness Analysis and Measurement* (pp. 3-30). Mahwah, NJ: Lawrence Earlbaum Associates.

Folker Jr., R. D. (2000). *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods*: Joint Military Intelligence College.

Gregoire, M., & Beaudoin, L. (2005). Visualisation for Network Situational Awareness in Computer Network Defence. *Meeting Proceedings RTO-MP-IST-043*, 20.21 - 20.26. Retrieved from http://www.rto.nato.int/abstracts.asp

Jones, M. D. (1995). *The Thinkers Toolkit*. New York: Three Rivers.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security, 28*(7), 509-520.

Lan, L.-n., Liu, X.-y., & Yang, T.-h. (2009, 10-11 July 2009). *Multi-layer and Multi-aspect Design of CA System Security.* Paper presented at the International Conference on Information Engineering, 2009 (ICIE '09), Taiyuan, Shanxi, China.

Li, J., Ou, X., & Rajagopalan, R. (2010). Uncertainty and Risk Management in Cyber Situational Awareness. In S. Jajodia, P. Liu, V. Swarup & C. Wang (Eds.), *Cyber Situational Awareness: Issues and Research* (pp. 51-67). New York: Springer.

Llinas, J., & Hall, D. L. (1998, 31 May-3 Jun 1998). *An introduction to multi-sensor data fusion.* Paper presented at the IEEE International Symposium on Circuits and Systems (ISCAS '98), Monterey, CA.

Mathew, S., Shah, C., & Upadhyaya, S. (2005, 23-24 March 2005). *An alert fusion framework for situation awareness of coordinated multistage attacks.* Paper presented at the Third IEEE Workshop on Information Assurance, College Park, Maryland.

Norman, D. A. (1990). The 'Problem' with Automation: Inappropriate Feedback and Interaction, not 'Over-Automation'. *Philosophical Transactions of the Royal Society of London. Series B, Biological Sciences, 327*(1241), 585-593.

Orlikowski, W. J., & Iacono, C. S. (2001). Research commentary: Desperately seeking "IT" in IT research - A call to theorizing the IT artifact. *Information Systems Research, 12*(2), 121-134.

Perrow, C. (1999). *Normal accidents : living with high-risk technologies : with a new afterword and a postscript on the Y2K problem*. Princeton, N.J.: Princeton University Press.

Salmon, P., Stanton, N., Walker, G., & Green, D. (2006). Situation awareness measurement: A review of applicability for C4i environments. *Applied Ergonomics, 37*(2), 225-238.

Shen, D., Chen, G., Haynes, L., & Blasch, E. (2007). *Strategies Comparison for Game Theoretic Cyber Situatational Awareness*. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA521036&Location=U2&doc=GetTRDoc.pdf.

Smith, K., & Hancock, P. A. (1995). Situation Awareness is Adaptive, Externally Directed Conciousness. *Human Factors, 37*(1), 137-148.

Stanton, N. A., Chambers, P. R. G., & Piggott, J. (2001). Situation Awareness and Safety. *Safety Science, 39*(3), 189-204.

Sudit, M., Stotz, A., & Holender, M. (2005, March 28). *Situational awareness of a coordinated cyber attack*. Paper presented at the SPIE Conference on Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security, Orlando, FL, USA.

Sudit, M., Stotz, A., Holender, M., Tagliaferri, W., & Canarelli, K. (2006). *Measuring situational awareness and resolving inherent high-level fusion obstacles*. Paper presented at the SPIE Conference on Multisensor, Multisource Information Fusion: Architectures, Algorithms, and Applications, Orlando, FL.

Tadda, G., Salerno, J. J., Boulware, D., Hinman, M., & Gorton, S. (2006, April 19). *Realizing situation awareness within a cyber environment*. Paper presented at the SPIE Conference on Multisensor , Multisource Information Fusion: Architectures, Algorithms, and Applications, Orlando, FL, USA.

Tadda, G. P., & Salerno, J. S. (2010). Overview of Cyber Situation Awareness. In S. Jajodia, P. Liu, V. Swarup & C. Wang (Eds.), *Cyber Situational Awareness* (pp. 15-35): Springer US.

Yang, S. J., Byers, S., Holsopple, J., Argauer, B., & Fava, D. (2008, June 17-20). *Intrusion activity projection for cyber situational awareness.* Paper presented at the IEEE International Conference on Intelligence and Security Informatics (ISI 2008). Tapei, Taiwan.

Yen, J., McNeese, M. D., Mullen, T., Hall, D. L., Fan, X., & Liu, P. (2010). RPD-based Hypothesis Reasoning for Cyber Situation Awareness. In S. Jajodia, P. Liu, G. Swarup & C. Wang (Eds.), *Cyber Situational Awareness: Issues and Research* (pp. 39-49). New York: Springer.

ADDITIONAL READINGS

Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective. *MIS Quarterly, 1*(3), 17-32.

Dennett, P. (1984). Cognitive Wheels: The Frame Problem of A.I. In C. Hookway (Ed.), *Minds, machines, and evolution : philosophical studies* (pp. 129-151). Cambridge [Cambridgeshire] ; New York: Cambridge University Press.

Durso, F. T., & Sethumadhavan, A. (2008). Situation Awareness: Understanding Dynamic Environments. *Human Factors: The Journal of the Human Factors and Ergonomics Society, 50*(3), 442-448.

Horton, K., Davenport, E., & Wood-Harper, T. (2005). Exploring sociotechnical interaction with Rob Kling: five "big" ideas. *Information Technology & People, 18*(1), 50.

Johnson-Laird, P. N. (2001). Mental models and deduction. *Trends in Cognitive Sciences, 5*(10), 434.

Johnson-Laird, P. N., & Savary, F. (1999). Illusory inferences: a novel class of erroneous deductions. *Cognition, 71*(3), 191.

McNeese, M. D., Bautsch, H. S., & Narayanan, S. (1999). A Framework for Cognitive Field Studies, *International Journal of Cognitive Ergonomics* (Vol. 3, pp. 307): Lawrence Erlbaum Associates.

Orlikowski, W. J. (2000). Using technology and constituting structures: A practice lens for studying technology in organizations. *Organization Science, 11*(4), 404-428.

Perry, M. (2003). Distributed Cognition. In J. M. Carroll (Ed.), *HCI Models, Theories, and Frameworks* (pp. 193-223). San Francisco: Morgan Kaufmann Publishers.

Salmon, P. M., Stanton, N. A., Walker, G. H., Baber, C., Jenkins, D. P., McMaster, R., et al. (2008). What really is going on? Review of situation awareness models for individuals and teams. *Theoretical Issues in Ergonomics Science, 9*(4), 297 - 323.

Sawyer, S., & Chen, T. T. (2002). Conceptualizing Information Technology in the Study of Information Systems: Trends and Issues. In M. D. Myers, E. Whitley, E. H. Wynn & J. I. DeGross (Eds.), *Global and Organizational Discourse about Information Technology* (pp. 1-23). London: Kluwer.

Scaachi, W. (2004). Socio-Technical Design. In W. S. Bainbridge (Ed.), *Berkshire Encyclopedia of Human-Computer Interaction*. Great Barrington, Mass.: Berkshire Pub. Group.

Suchman, L. A. (1987). *Plans and situated actions : the problem of human-machine communication*. Cambridge [Cambridgeshire] ; New York: Cambridge University Press.

Weick, K. E., Sutcliffe, K. M., & Obstfeld, D. (2005). Organizing and the Process of Sensemaking. *Organization Science, 16*(4), 409.

Woods, D. D., & Patterson, E. S. (2000). How unprecedented events produce an escalation of cognitive and coordinative demands. In P. A. Hancock & P. A. Desmond (Eds.), *Stress, workload, and fatigue* (pp. 112-136). Mahwah, N.J.: Lawrence Erlbaum Associates, Publishers.

Young, M. F., & McNeese, M. D. (1995). A situated cognition approach to problem solving. In J. Caird, J. Flach, P. A. Hancock & K. Vincent (Eds.), *Local applications of the ecological approach to human-machine systems* (pp. 359-391). Hillsdale, N.J.: L. Erlbaum.

KEY TERMS AND DEFINITIONS

Algorithmic Perspective: An analytical perspective technology and the use of technology in which technology is limited to software and hardware and the human-actor is excluded.

Cognition: Mental processes including attention, perception, comprehension, learning, problem-solving, and memory.

Cyber Situation Awareness (Cyber-SA): A form of situation awareness specific to the cyber-security context. Cyber-SA is distinguishable from situation awareness in that it occurs in an entirely virtual hyper-dynamic information-intensive context.

Cyber-security: The practice of monitoring and security networked computer and information assets to prevent unauthorized access, modification, or service denial.

Risk Space: A *n*-dimensional matrix in which risk vectors are plotted for the purpose of predicting the degree of risk in a particular setting.

Situation Awareness: The cognitive process by which a human actor perceives and understands environmental cues in relation to a specific task context. A human actor who has correctly comprehended the environmental state and subsequently established the correct task goal has achieved the state of situation awareness.

Structured Analysis: Formal methods of analytical thinking designed to reduce or eliminate the effect of analyst bias and produce more accurate analyses.