Chapter 18
An Alternative Framework for Research on Situational Awareness in Computer Network Defense

Eric McMillan
The Pennsylvania State University, USA

Michael Tyworth
The Pennsylvania State University, USA

ABSTRACT

In this chapter the authors 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, the framework in this chapter presents a basis for examining cyber-SA at the cognitive, system, work, and enterprise levels of analysis. In describing the framework, the authors 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

DOI: 10.4018/978-1-4666-5942-1.ch018

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 (Figure 1) 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.