Chapter 1
Review of Situational Awareness for Computer Network Defense

Cyril Onwubiko
Research Series Limited, UK

Thomas John Owens
Brunel University, UK

ABSTRACT

The importance of situational awareness to air traffic control, and hence the safety and security of aircraft, is evident, demonstrable, and has been hugely significant. The main purpose of this book is to convey an understanding of the impact of situational awareness on the design of the next generation computer systems, network architectures, and platform infrastructures. The book achieves its purpose by presenting principles, methods, and applications of situational awareness for computer network defense; in doing so, it makes clear the benefits situational awareness can provide for information security, computer security and computer network defense. This book contributes to cross-multidisciplinary discussion among researchers, academia, and practitioners who are engaged objectively in sharing, contributing, and showcasing how situational awareness can be adapted to computer systems, network infrastructure designs, and architecture patterns. The goal of this chapter is to explain situational awareness for computer network defense from the point of view of its most basic foundations as a spring board to discuss how situational awareness can be relevant to computer network defense, whose operations and environment are similar to air traffic control where the application of situational awareness has been hugely successful.

SITUATION AWARENESS

Situation awareness (SA) is made up of two words ‘situation’ and ‘awareness’. According to Chambers 21st Century Dictionary (Chambers, 1997), Situation (noun) is defined as:

1. A set of circumstances or state of affairs.
2. A place, position or location.
3. A job; employment. Example, situations vacant.
4. A critical point in the action of a play or in the development of the plot of a novel.
Situational is *adjective of situation*. ETY-MOLOGY: 15c. *Awareness* (noun) is defined as the fact or state of being aware, or conscious, especially of matters that are particularly relevant or topical (Chambers 1997). Putting these two words together, we define *Situational Awareness* as the state of being aware of circumstances that exist around us, especially those that are particularly relevant to us and which we are interested about. By this definition, situational awareness means, as people, we seek to be aware of situations around us, particularly those that we are interested in. For example:

- Every driver wants to know about obstacles along their way, especially those that may lead to an accident. For instance, when reversing, drivers usually look into the rear and side mirrors of their car to ensure they are aware of any impeding situation, for instance objects, or obstacles, or onward moving vehicles so as to be apprised of the risk of such situations and avoid them.
- A nursing mother wants to maintain situational awareness of the environment which her crawling baby is in, especially; she wants to keep the baby away from any objects that can be of harm to the baby such as breakable (glass) cups, scissors, photo frames, table knives, etc.
- Politicians want to be aware of how popular their government is, for instance, by checking what the polls say. Moreover they do this especially when new legislation or bills have been passed.
- In computer network security and information security organizations want to be aware of the vulnerabilities of their assets and weaknesses that may exist in the mechanisms used to protect their assets, and the risks that may result should vulnerabilities be exploited. More importantly, organizations want to know about the vulnerabilities of assets which if exploited could have a significant or even catastrophic impact on the organization.
- In computer network defense the mission (agency or organization) wants to be aware of the vulnerabilities that may exist in its systems and any weakness that may exist in the systems defense controls, including possible threats and threat actors (such as, foreign intelligence services) that may be interested in compromising, breaching or circumventing its defense systems and wants to be aware of the motivation and capability of such threat actors.

**Evolution of SA Definitions**

Recorded accounts of SA definitions began in the mid 1980s, but the use of the term ‘SA’ can be traced back to World War I. This is not surprising, because as one samples through some of the existing SA definitions in the literature, one realizes that situational awareness’s foundational development stems from psychology, human factors and military warfare operations. For example, Hamilton 1987, Endsley 1988, Regal et al. 1988, Beringer and Hancock 1989, Taylor 1990, Carol 1992, Vidulich 1994, Billings 1995, and Endsley 1995 all defined SA in relation to human factors, pilots, aviation, warfare and air traffic control (ATC).

A general purpose definition of SA, we believe, was provided in 1998. According to Endsley (1998), SA describes “the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future”. This definition has become the most quoted, cited and accepted definition for situational awareness, alongside Endsley’s (Endsley 1995b) proposed abstract model for situation awareness (See Figure 1) which has since been extended by McGuinness and Foy (2000) to include a fourth level of situational awareness called *Resolution*. 