Review of Situational Awareness for Computer Network Defence

Cyril Onwubiko
Intelligence & Security Assurance, Research Series Limited, London, United Kingdom

Thomas John Owens
ECE School of Engineering and Design, Brunel University, United Kingdom

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*. **ETYMOLOGY:** 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*.

It was not until recently that the application of SA to Cyber security, information security, network computer security and computer network defence (CND) began to emerge, Grégoire and Beaudoin, 2005, Lefebvre et al, 2005, Onwubiko, 2009, Jajodia et al. 2009, and Barford et al, 2009.

Figure 1 is adapted from Endsley's situation awareness reference model (Endsley, 1995b), which presents three levels of situation awareness, *perception*, *comprehension* and *projection*. In addition McGuinness and Foy’s (2000) extension of Endsley’s SA model includes *resolution* as a fourth level of situation awareness.

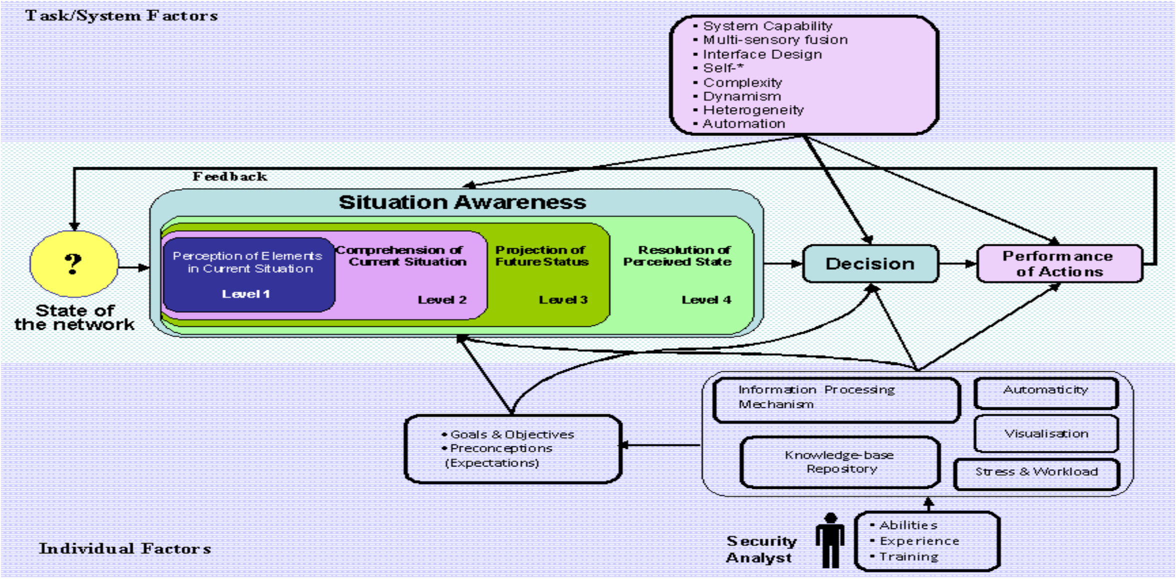

Figure 1: Network Security Situation Awareness Model (Onwubiko, 2011b)

- *Perception* is regarded as Level 1 SA. In relation to CND, perception refers to knowledge of the elements in the network that security analysts (operators) must be aware of, such as alerts reported by intrusion detection systems, firewall logs, scan reports, as well as the time these pieces of security evidence occurred and the specific controls that reported the alerts or generated the logs (Onwubiko, 2009). Perception also relates to observed and unprocessed low-level data. According to Salerno et al (2004), *perception* provides information about the status, attributes and dynamics of the relevant elements in the environment. It extends the classification of information into meaningful representations that offer the basis for comprehension, projection and resolution.

- C*omprehension* is regarded as Level 2 SA. To understand the true nature of the perceived threats, and ascertain the threat level, security logs and alerts must be analysed, assessed and synthesized. At the comprehension level, a number of techniques, methodologies, processes and procedures are used by security analysts to analyze, synthesize, correlate and aggregate pieces of evidence perceived in the network in order to deduce the level of perceived threats or to determine if the network has been compromised. Hence, c*omprehension* involves a determination of the relevance of the pieces of evidence captured to the underlying goal of resolution of the situation (Salerno et al, 2004). Thus, comprehension offers an up-to-date picture of the current situation by determining the significance of the evidence perceived together with the importance of the assets being monitored so that when new sets of evidence become available the knowledge-base is updated to reflect this change (Onwubiko, 2009).

- *Projection* is regarded as Level 3 SA. It refers to the ability to make predictions or forecasts based on the knowledge extracted from the dynamics of the network and comprehension of the perceived situation (Onwubiko, 2009). Hence, it implies the responsibility of the security analyst (operator) to forecast future events, or predict patterns of occurrence of future events based on pieces of evidence synthesized from low level SA (Levels 1 & 2). This enables decision makers and security analysts to forecast future network states and provide preventive controls to address potential situations. In this respect, *Projection* tries to answer questions such as, what network attacks are possible on our network? And what controls may be needed to address, prevent, or respond to such attacks should vulnerabilities be exploited?

- *Resolution* is regarded as Level 4 SA. It refers to applicable and possible countermeasure controls required to manage risks inherent in or dependent on the networks being monitored. *Resolution* was first discussed in situation awareness by McGuinness and Foy, 2000 as an extension to Endsley's SA abstract model. Resolution is concerned with the provision of the necessary actions and controls required to resolve a perceived network situation.

These terms (*perception, comprehension, projection* and *resolution*) are discussed in this chapter in relation to situational awareness for computer network defence (Cyber SA).

In summary, *perception* deals with the gathering of evidence of situations in the network, *comprehension* deals with the analysis of sets of evidence to deduce exact threat levels, types of attack and associated or interdependent risks. *Projection* deals with predictive measures to estimate future incidents, and *resolution* deals with controls to repair, recover and resolve network situations.

SITUATIONAL AWARENESS FOR COMPUTER NETWORK DEFENSE

Cyber situational awareness (Cyber SA), computer network defence situational awareness (CND SA), and network security situational awareness (NSSA) are some of the newly emerging terminologies used to express the application of SA to the wider information security domain.

Situational awareness is described as knowing what is going on around you and with that knowledge of your surroundings being able to identify which events in those surroundings are important. SA is very complex and involves very dynamic states, e.g. of a computer network with hundreds of network objects (firewalls, IDSs, routers, switches, servers, PADs etc). Maintaining a consistently high level of situational awareness over these objects can be challenging (Onwubiko and Owens, 2010). Thus, the underpinning of situational awareness in computer networks is to assist operators to identify adversaries, estimate impact of attacks, evaluate risks, understand situations and make sound decisions on how best to protect valued assets swiftly and accurately (Onwubiko, 2009). By this proposition, we believe that, the application of SA to CND will yield unprecedented benefits akin to SA for safety and security in aircraft, flight operation, ATC and safety controls.

In many respects, SA is comparable to the OODA (observe, orient, deduce and act) loop (Onwubiko, 2011b). The OODA decision control was first proposed by Boyd, (1987) for use in Command and Control (C2) environments. This means operators need to observe network situations, evaluate the situation, deduce the impact it may have and decide possible mitigation controls to effectively and accurately address the situation. By continually following the OODA loop, an operator or group of operators are able to act in accordance to the situation they are in. The operator may use technology, in this case protective monitoring, interfaces, HCI interactions, and other methods, (see Onwubiko, 2011b) to enhance situational awareness of the network being monitored and then decide the best possible cause of action to be taken.

Whether SA or OODA, the approach for CND is:

- First, the network should be monitored by trained and experienced network security operators;
- Second, these operators through the use of tools and technologies are able to observe, analyse and resolve abnormal situations (faults, errors and attacks) in the network;
- Third, operator SA is enhanced through the use of technologies that are swift and accurate in processing and analysis of perceived situations in networks. Thus, operators gain enhanced situational awareness of the environment by monitoring networks and ensuring network activities (alerts, logs, volumetric statistics and abnormal behaviour) are visualised, whilst using techniques (correlation and fusion techniques) that are able to combine and analyze data from a number of distributed sensors deployed in and around the network;
- Fourth, using their mental models (past knowledge of network behaviours, experience and training) operators are able to make projections about future network states. For example, based on observed network traffic and volumetric statistics an experienced operator could make an accurate estimation of when the network is under attack from an evolving computer worm mutant or variants of self-propagating malicious code.

BACKGROUND

Computer crimes around the world cost organisations and governments billions of dollars each year. In response, organisations use a plethora of heterogeneous security devices and software such as firewalls, Intrusion Detection Systems (IDS), Security Information and Event Management (SIEM) to monitor networks in conjunction with Computer Security Incident Response Teams (CSIRT), that are responsible for ensuring availability, integrity and confidentiality of network services. Their primary challenge is to maintain situational awareness over many critical network objects some of which include critical national infrastructures, the impact of a cyber attack on which could result in a breakdown in national communications networks or essential support services, which may impact on citizens’ safety or livelihoods. Maintaining consistent high-level situational awareness over such objects requires that the CSIRT has the knowledge and ability to perceive and analyse situations that may have security related implications, make sound decisions on how to protect organisations' valued assets and offer accurate predictions of future states in dynamic and complex environments. This is the underpinning of situational awareness in computer network defence (Onwubiko, 2009).

In the last fifteen years the application of SA has been revolutionary, particularly in ATC, Defence and Military operations where SA has been extensively researched. ATC operation, for instance, can be compared to CND operation; unfortunately, while the application of SA to CND is still in its embryonic stage, its application to ATC is mainstream (Onwubiko, 2009).

COMPUTER NETWORK DEFENSE

Cyber attacks on computer networks are growing and evolving. For example, from code-driven attacks, deliberate malicious software attacks, espionage, distributed denial of service attacks, phishing to the recent computer electronics attacks, such as Stuxnet. All these contribute to demonstrate how complex and challenging the CND environment is (Onwubiko, 2008).

CND is a growing field which is geared towards measures to protect and defend computer networks and information systems from cyber attacks that could cause disruption, denial of service, degradation and destruction (Onwubiko and Owens, 2010). A CND environment is one that ensures that vulnerabilities that exist in computer networks are addressed, threats to the environment are identified and controls and risks inherent to this environment are managed to an acceptable level in relation to the organisation (Onwubiko, 2011b).

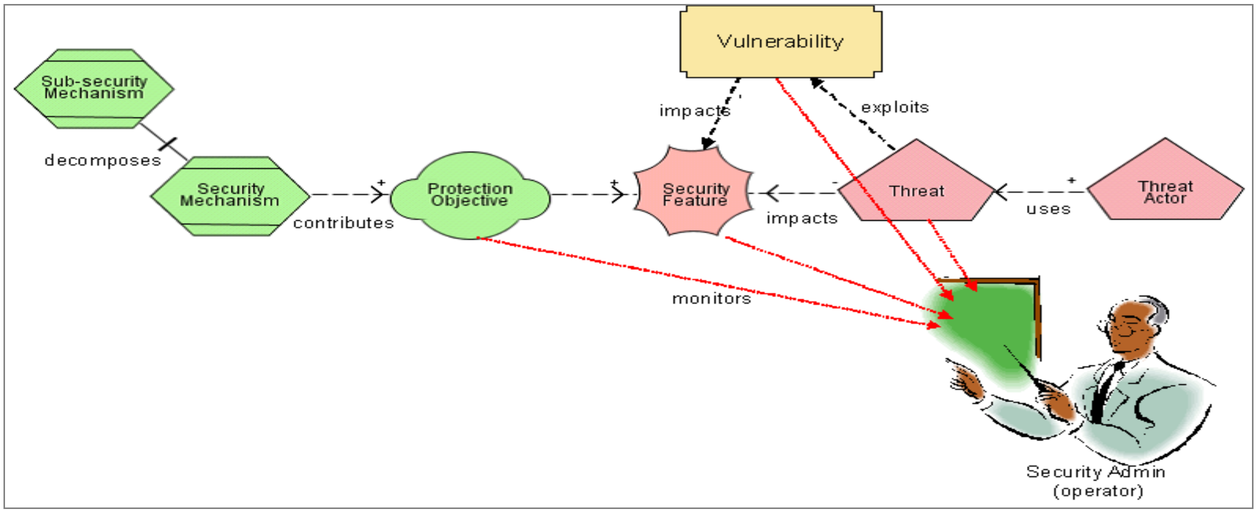

Figure 2: Operator monitors a CND Environment

Figure 2 is a basic model of a CND environment. It shows that security mechanisms (such as a firewall) can be decomposed into several sub-security mechanisms, such as an access control list (ACL), and that the security mechanisms contribute to achieving the protection objectives (such as allow only authorised access). However, security threats can lead to the compromise of or breach of security features by threat actors exploiting vulnerabilities that may exist in assets. The security administrator (operator) who monitors the CND environment must maintain situational awareness over these systems, which in itself is demanding and challenging, however, the operator shall assess the existence of vulnerabilities in the protection of assets, and whether existing vulnerabilities can be exploited. The operator must check if protection objectives are achieved, and whether security features can be breached, compromised or violated. Finally, the operator must assess the impacts threats may have should a security attack be realised.

One of the primary purposes of CND is to ensure that systems and networks are secure, reliable and operational. This includes actions taken via computer networks to protect, monitor, analyse, detect and respond to cyber attacks, computer network intrusions, disruptions or other perceived unauthorized actions that could compromise or impact network defense and information systems. CND is achieved through a collective effort by personnel (a.k.a. 'human' operators) who monitor, manage and maintain defence systems, networks and infrastructures, such as network operators, security analysts, systems administrators and network engineers. These personnel are faced with the onerous tasks of coordinating, maintaining, monitoring and ensuring the necessary actions required in keeping defence systems and network infrastructures operational, whilst ensuring that appropriate protection from cyber-attacks is provided on a daily basis (Onwubiko, 2011).

Table 1: ATC compared to CND

FEATURES	ATC	CND
Human operator	Service is provided by ground-based controllers (human operators) who direct aircraft on the ground and in the air	Service is provided by security analysts (human operators) who monitor systems and networks for abnormal traffic, behaviour, signs, events and alerts
Goal	Primary goal is to prevent aircraft collisions, organize and expedite the flow of traffic and to provide information and other support to the pilot when required	Primary goals are to ensure systems and networks are protected, and services are availability to users or consumers when required.
Activities	Requires information of varying nature ranging from weather information to longitudinal and latitudinal information (location information)	Requires information on the ICT systems being infected, and the sensors or defence systems that detected the issue. For example, an IDS (intrusion detection system) detected an intrusion against a critical asset
Information	Issue instruction that pilots are required to follow or mere flight advisory to assist pilots operate in the airspace	Provide information to the organisation (security manager) about perceived threat level, on-going attacks and risks, so that the manager can advise on CoA (cause of action)
Security	Provide security or defence role to the aircraft	Provide security and defence function for the organisation by ensuring alerts, event and attacks are identified, addressed and resolved.
Use of Technology	Uses collision avoidance systems, GPS (global positioning systems), GIS	Uses IDS, firewall, AV (anti-virus), sensors, guards file and log integrity

	(Geographic information systems), GNSS (Global Navigation Satellite System) and location tracking and monitoring systems to inform the pilot of changing weather conditions, incoming aircraft and navigation information and NOTAMs (NOtices To Air Men)	violation tracker and security event and information monitoring systems to monitor the systems and networks
Environment	Usually dynamic and complex in nature involving the monitoring and coordination of various activities such as weather information, collision avoidance information, ground-based activities and air-based activities, which require swift and instantaneous response	Usually dynamic and complex in nature. Involving monitoring of a myriad of toolkits used to monitor the network such as protective monitoring of servers, traffic utilisation, network traffic (normal and abnormal), threshold and threat and vulnerability advisories including intelligence about threat actors.
Coordination	Controller coordinates numerous other operators who assist to ensure that the ATC operations are successful, such as GIS technicians, backroom and backoffice operators, pilots, flight crews etc.	Security analysts work with security administrators, network engineers, system support and IT support to ensure that systems and network infrastructure of the mission is protected.
Impact	Failure to coordinate ATC operations and activities leads to significant impact, first aircraft will not be allowed to fly, and those already in the air may witness severe disruption in service and accidents may occur as a result.	Failure to monitor network and systems will impact the organisation as security incidents may not be resolved, this may impact service level agreements, resulting in significant financial penalties, and consequently putting the network at risk.

CONCLUSION

The goal of this chapter is to explain situational awareness for computer network defense from the point of view of its foundations and use this as a spring board to discuss how SA can be relevant to CND whose operations and environment are similar to ATC where the application of SA has been hugely successful.

REFERENCES

Barford P., Dacier M., Dietterich T. G., Fredrikson M., Giffin J., Jha S., Li J., Lui P., Ning P., Ou X., Song D., Strater L., Swarup V., Tadda G., Wang C., and Yen J., (2009). Cyber SA: Situational Awareness for Cyber Defense, in Cyber Situational Awareness: Issues and Research (Advances in Information Security), (Eds) S. Jajodia, P. Liu V. Swarup and C. Wang

Boyd J., (1987). Organic Design for Command and Control. Presentation Slides, May 1987 [Accessible from] www.ausairpower.net/JRB/organic_design.ppt

Chambers Dictionary (1997). Chambers 21st Century Dictionary. [Accessible from] http://www.chambersharrap.co.uk/chambers/features/chref/chref.py/main

Endsley M. R., (1995b). Toward a Theory of Situation Awareness in Dynamic Systems. Human *Factors Journal,* ***Vol. 37, No. 1, pp. 32-64****, 1995.*

Endsley M. R., (2000). Errors in Situation Assessment: Implications for System Design. In P. F. K. R. H. B. B. Elzer (Eds), *Human Error and System Design and Management (Lecture Notes in Control and Information Sciences Vol. 253, pp 15-26,* Springer-Verlag, London, UK, 2000.

Grégoire M., and Beaudoin L. (2005). Visualisation for Network Situational Awareness in Computer Network Defence; In *Visualisation and the Common Operational Picture* (pp. 20-1 – 20-6); Meeting Proceedings RTO-MP-IST-043, Paper 20; Neuilly-sur-Seine, France, RTO, 2005.

Jajodia S., Liu P., Swarup V., and Wang C. (eds.) (2009). Cyber Situational Awareness: Issues and Research (Advances in Information Security), Springer, ISBN 1441901392, 2009.

Lefebvre J. H., Grégoire M., Beaudoin L., and Froh M. (2005). Computer Network Defence Situational Awareness *Information Requirements,* Defence R&D Canada – Ottawa, Technical Memorandum, DRDC Ottawa TM 2005-254, December 2005.

McGuinness and L. Foy, (2000). A Subjective Measure of SA: The Crew Awareness Rating Scale (CARS). *Proceeding of the First Human Performance, Situation Awareness, and Automation Conference, Savannah, Georgia, 2000*.

Onwubiko, C., (2008), "Data Fusion in Security Evidence Analysis”**;** Proceeding of the 3rd International Conference on Computer Security and Forensics, 2008.

Onwubiko C., (2008). Security Framework for Attack Detection in Computer Networks. VDM Verlag, ISBN 978-3-639-08934-9, 2008.

Onwubiko C., (2009). Functional requirements of situational awareness in computer network security, *IEEE International Conference on Intelligence and Security Informatics*, ISI '09, Dallas, TX, USA, 8-11 June 2009.

Onwubiko, C., and Owens, T.J., (2010). Call for Chapters: Situational Awareness in Computer Network Defence: Principles, Methods and Applications, IGI-global, USA, 2010 [Accessible from] http://www.wikicfp.com/cfp/servlet/event.showcfp?eventid=11783&copyownerid=16539

Onwubiko, C. (2011). Modeling Situation Awareness Information and System Requirements for the Mission using Goal-Oriented Task Analysis Approach. In C. Onwubiko and T.J. Owens (Eds.) *Situational Awareness in Computer Network Defense: Principles, Methods and Applications*.

Onwubiko, C. (2011b). Designing Information Systems and Network Components for Situational Awareness. In C. Onwubiko and T.J. Owens (Eds.) *Situational Awareness in Computer Network Defense: Principles, Methods and Applications*.

Salerno, J, Hinman, M. and Boulware, D., (2004). Building a Framework for Situation Awareness, AFRL/IFEA, AF Research Lab., Rome, NY 13441-4114, USA, 2004.

Tadda, G. P., and Salerno, J. S. (2009). Overview of Cyber Situation Awareness, in Cyber Situational *Awareness: Issues and Research (Advances in Information Security), Springer* ISBN: 1441901392, 2009.

Wang H., Liu X., Lai J., Liang Y., (2007). Network Security Situation Awareness Based on Heterogeneous Multi-sensor Data Fusion and Neural Network, *Second International Multi-Symposiums on Computer and Computational Sciences,* IMSCCS 2007, pp.352-359, 2007.