Understanding Cyber Situation Awareness

Cyril Onwubiko

Centre for Multidisciplinary Research, Innovation and Collaboration (C-MRiC.ORG), London, UK

ABSTRACT

Historically, situation awareness has been applied to mainstream disciplines such as psychology, air traffic control, and aviation. This trend has since changed. Situation awareness has expanded now into the Cyber domain such as social media, vehicular networks (VANET), cybersecurity, CERTs and computer network defense (CND) etc. With every new innovation or its application, there is potential for misconceptions, misinterpretation and downright misunderstanding. This has led to situations where very many ‘things’ have now been ‘branded’ Cyber SA, many of which have nothing to do with situation awareness. This paper introduces Cyber SA, provides definitions, examples and discusses applications of situation awareness in the Cyber domain.

Keyword: Cyber Situation Awareness, Cyber SA, Situation Awareness, Computer Network Defense, Situational Awareness, SA, CND, Cybersecurity, VANET, CERT, SOC, Cyber SA Applications

1 INTRODUCTION

It is evident that the use of the phrase ‘Cyber situation awareness’, ‘Cyber situational awareness’ or Cyber SA is on the rise. A search for ‘Cyber situation awareness’ on Google showed over 5 million results in 0.25 seconds (Google, 2016). This is phenomenal. The use of the phrase is one thing, but what might be interesting is to understand some of the underlying factors behind its rise.

One factor that could account for this widespread use is the application of situation awareness in mainstream disciplines, and more recently, into emerging disciplines such as social media, vehicular networks (VANET) and cybersecurity. For instance, situation awareness has been well-studied and applied to several mainstream disciplines, such as psychology, aviation control, medicine, ground transportation, maintenance, space and military operations since the seminal work of Endsley (Endsley, 1995). Most recently, that is, in the last fifteen years or so, the application of situation awareness has been revolutionary, particularly in air traffic control (ATC), defence and intelligence operations, weather forecast and road transportation systems (Endsley, 2000, Onwubiko, 2009). Further, it has now been expanded into the emerging Cyber domain such as CERTs, VANETs, social media and cybersecurity. For instance, there are now notable accounts of the application of SA to Cyber security, information security, security operations centres (SOC), computer network defence, intelligence and fusion centres (Grégoire & Beaudoin, 2005, Lefebvre et al, 2005, Onwubiko, 2009, Jajodia et al. 2009, Barford et al, 2009, Onwubiko, 2015, Onwubiko, 2016 and Eiza, Owens & Ni, 2016).

The increasing and evolutionary nature of recent Cyber-attacks and threats that appear to exploit vulnerabilities that exist in computer networks, critical national and business infrastructures have meant that new and emerging approaches to conventional methods are now sought. So as industry, government and academia seek new and reliable approaches to addressing recent cybersecurity issues, Cyber SA is seen as a frontier.

The problem with this is that very many ‘things’ have now been ‘badged’ Cyber SA, many of which have nothing to do with situation awareness. Therefore, the primary focus of this chapter is to describe what situation awareness is in the context of Cyber domain. This work builds upon our earlier contributions (Onwubiko, 2009, Onwubiko, 2011, Onwubiko & Owens, 2011, Onwubiko, 2015, and Onwubiko, 2016).

The remainder of this chapter is organised as follows: Section 2 discusses situation awareness in general, while in section 3 Cyber SA is defined, explained and its application demonstrated. Section 4 describes examples of Cyber SA applications, while section 5 outlines some misconceptions, and the chapter concludes in section 6.

2 SITUATION AWARENESS

According to Endsley, SA is simply defined as *knowing what is going on around you*. A definition she expanded as "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" (Endsley, 1988). This definition crystallizes SA to comprise three distinctive aspects – Perception (*awareness of current situation with respect to time*), Comprehension (*understanding of the current situation, consequences, impacts, changes in the situations over time, and possibly what could have caused it*) and Projection (*estimation of the changes in the current state, and what could become of the impending situation if not controlled in time, and prediction of possible evolution of the current to impending situation*).

Over the years, SA has been defined in a number of complementary ways, most focusing on the application of SA to specific domains. For example, Cumiford defines SA in Cyber Defense as the *ability to rapidly and effectively address incoming stimuli with appropriate response* (Cumiford, 2006); while others have added dimensionality to existing definitions. For instance, McGuinness and Foy extended Endsley's SA model to include *resolution* as the level four situation awareness component (McGuinness & Foy, 2000).

In general, SA is defined 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* (Onwubiko & Owens, 2011). According to the authors "situation awareness means, as people, we seek to be aware of situations around us, particularly those that we are interested in (context), and at that particular moment (time)". Each situation may be different and what is considered important is likely to be different, too.

Here are some examples to explain some situations, and the needed awareness in respect of the situation by the operator or organisation:

a) Every driver wants to know about obstacles along their way, especially those that may lead to an accident at the time. For instance, when reversing, drivers usually look into the rear and side mirrors of their car or/and the dashboard to use the camera to see close objects, and further, for the most recent cars, use sensors to track proximity of another car or object to ensure they are aware of any impeding situation, objects, or obstacles, or onward moving vehicles so as to be apprised of the risk of such situations and avoid them.

b) A nursing mother wants to maintain situation 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. and may use room monitors to observe the baby, and including audio room sensor to alert her when the baby is near to objects that may cause harm to the baby.

c) Politicians want to be aware of how popular their government is, for instance, by checking what the polls say, correlating opinion polls, and may conduct surveys and use social media to gauge popularity etc. Moreover they do this especially when new legislation or bills have been passed or during periods leading up to a general election.

d) With computer network or information security, organisations 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, organisations want to know about the vulnerabilities of assets which if exploited could have a significant or even catastrophic impact to the organisation.

e) With computer network defense, the mission (agency or institution) wants to be aware of the vulnerabilities that may exist in its systems and any weakness that may exist in the defense controls, including possible threats and threat actors (such as, hostile foreign intelligence services) and nation state 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.

f) With Cyber (which in this article encompasses (d) and (e) above), the institution (e.g. academia, industry and government) wants to gain understanding of threats to their digital assets, the vulnerabilities that exist within the assets and controls being used to protect the assets, and potential incidents that could occur and what risks this may possess and what countermeasures may be needed to address the perceived risks. Understanding can be gained through a number of different controls, such as monitoring digital services, users of such services, transactions originated to and from various geographies; and enforcement of policy compliance and regulatory directives. Gaining intelligence of threat posture and potential attacks, possible cause of action, and required countermeasures.

3 CYBER SITUATION AWARENESS

Cyber SA is the application of situation awareness in Cyber domain. Cyber is a very complex and diverse domain comprising many aspects, most of which involve extremely complex, challenging and dynamic states. Take for example, online web transactions involving various entities from various geographies, none of which is static.

Situation awareness is derived from many sources of information and cues may be received from visual, aural, tactile, olfactory or taste receptors (Endsley & Garland, 2000). This means mechanisms or media through which meaningful cues can be obtained are considered extremely useful in SA. For example, cues can be rendered in realtime to operators through a visual dashboard that combines video images, analytical graphs, charts, audio and textual information in a coordinated fashion to provide, and arguably enriched the operators' situation awareness. Multimedia is considered an important component of any SA technology.

In principle, Cyber SA is no different to the application of situation awareness to other domains, such as SA in ATC or SA in ground military operations. The need for SA in Cyber can be demonstrated by the following problem statements:

a) Imagine an organisation's computer network with hundreds or thousands of network objects (e.g. firewalls, IDSes, routers, switches, servers, desktops, laptops, PADs, tablets, smartphones etc.), and thousands of privileged users – internal and partners, and processing millions of transactions and generating terabytes of logs daily. Monitoring and managing such an enterprise is likely to be challenging. Example of such an enterprise is a multinational company.

b) Imagine an online ecommerce portal processing millions or thousands of millions of both web and financial transactions daily. Monitoring and manging such an enterprise is likely to be challenging, e.g. Amazon, eBay, etc.
c) Imagine an online financial services institution handling millions of high value-bearing transactions daily from across various geographies; in addition to adherence to financial services regulations and compliance directives. Monitoring and managing such an enterprise is likely to be challenging, e.g. a financial institution, a bank etc.
d) Finally, imagine a government agency monitoring millions or billions of citizens' assets, national critical infrastructures, and responsible for protecting citizens both in the country and abroad. Managing such an enterprise is likely to be challenging, e.g. Foreign and Commonwealth Office, or Homeland Security.

The above scenarios and many more use cases require understanding of a number of different situations, an awareness of, comprehension thereof, projection of current situation, and the estimation of escalations of current situations to impending future situations, and resolution of both the current situations and the impending ones. Understanding and/or resolution of these situations could not happen without the people – analysts, administrator, operators etc., who know, monitor and manage the systems, hence Cyber SA will be incomplete without operators. People are an integral aspect of Cyber SA.

In summary, Cyber SA encompasses people (operator/team), process and technology required to gain awareness of historic, current and impending (future) situations in cyber, the comprehension of such situations, and using those understandings to estimate how current situations may change, and through those predict future situations and the resolution of the current situation, and the enablement of controls to protect the systems from future projected incidents.

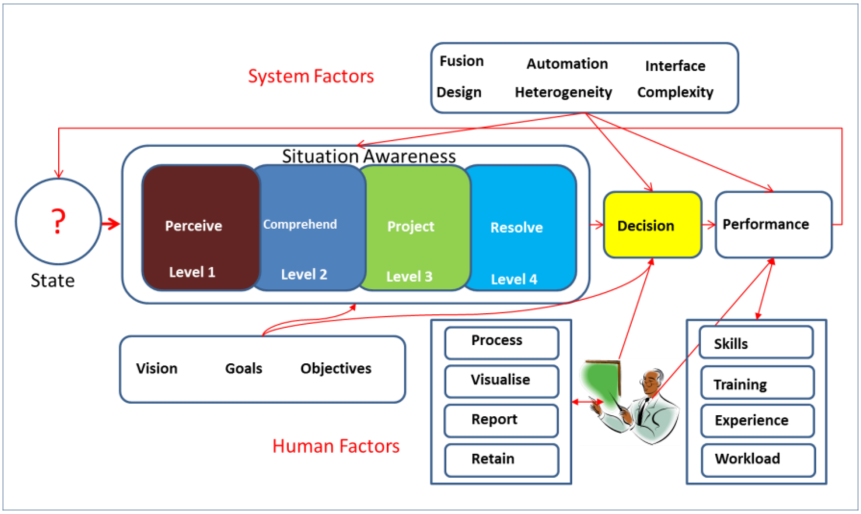

FIGURE 1: SITUATION AWARENESS REFERENCE MODEL

Figure 1 is adapted from Endsley's situation awareness reference model (Endsley, 1995), which presents three levels of situation awareness, *perception*, *comprehension* and *projection*. It has incorporated McGuinness and Foy's extension of Endsley's SA model that includes *resolution* as the level four situation awareness component (McGuinness & Foy, 2000); and further refined and presented in (Onwubiko, 2012).

These terms (*perception*, *comprehension*, *projection* and *resolution*) are discussed in this chapter in relation to Cyber. *Perception* deals with evidence gathering of cyber situations, *comprehension* is related to understanding of the exact situation, which may be derived from analysis of the set of evidence gathered or perceived of the current cyber situation, and also involves the understanding of the exact threat level, identification of attack types, and of the associated or interdependent risks. *Projection* deals with predictive measures to forecast future incidents, situations or states using current state of the situation, and understanding of how current situations could escalate. In addition, it relates to estimation of, and what the current situation could become in the nearest future considering the perceived current tension, escalations and evolution that might happen over time. Finally, *resolution* deals with controls to repair, recover, remedy and resolve the perceived cyber situations.

Systems factors are technology-enabled features, mechanisms or techniques that help the operator receive system-specific cues such as fusion, automation, interfaces, design, integration and architecture (see Figure 1). For example, when monitoring a network, the organisation may deploy a number of technologies to detect cyber-related situations, such as, sensors to detect cyberattacks, scanners to identify vulnerabilities that exist in their systems, intrusion detection systems to detect policy deviations etc. Pieces of evidence from these technologies will need to be fused/combined allowing correlation of event from disparate systems to happen, using electronic interfaces capable of real-time transmission, and the capability to analyse, process and assess information from heterogeneous sources. System factors are system-specific tasks and requirements that assist individuals/operators gain situation awareness swiftly. They contribute at different levels of the SA model (*L1-L4*), and help inform decision making by the operator and could improve operator performance too. For instance, providing accurate evidence of system compromise at pace can improve both decision making, and performance or speed of response recommended by the operator.

The *vision, goals and objectives* drive the level of investment that the organisation may be willing to make in an effort to protect their valued assets; most importantly, the objectives will drive the risk appetite and risk tolerance of the organisation, while goals will be used as a measure of success to assess the return on investment.

Human factors are individual or group (a.k.a. team situation awareness) attributes that enhance or impact operator situation awareness, such as skills, experience, abilities and training (SEAT). Likewise, environment, workload and stress do affect the individual's capacity to perform his/her job, hence influencing both quality and performance. The operator or the team should have the skills and experience to analyze, assess and process cues being provided to them in order to produce appropriate reports, and determine cause of actions in addressing the issues; this includes the skills and knowledge to use specialist techniques, tools and technology to manipulate and synthesize data and information in order to gain enhanced intelligence.

Decision is the operator responsibility, which will be informed through a number of different inputs. For instance, decisions can be reached by determining accurately the causes of action (CoA), understanding of exact issues, which then informs appropriate actions to be executed. Tools and technology are used to synthesis, analyse and process cues, information and intelligence to arrive at a conclusive set of response. It is important to note that 'a conclusive set of response' are not always arrived at in every situation. This is because some evidence may be incomplete, contradictory, and at times, conflicting, so decision making in itself can be challenging at times.

Decision takes multidimensional inputs in order to recommend a set of responses to be actioned as shown in Figure 1. It takes input from system factors, considers evidence of analysis outcome of threat intelligence feeds, in consideration of the vision, goals and objectives of the business. Further, it uses the reports provided by the experts/operators in order to decide the most appropriate action to take to address the situation or situations.

3.1 Understanding Cyber Situation Awareness

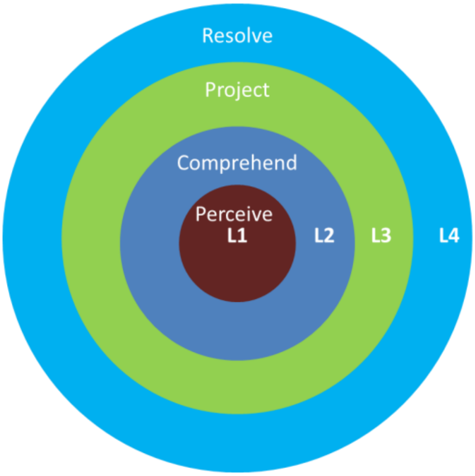

FIGURE 2: CORE SA / LEVELS

Cyber SA levels are represented in this research as concentric circles. The rationale for representing them this way is to show the interconnectedness and dependences among them (see Figure 2). This means that Cyber SA exists at different levels – i.e. Level 1 – Level 4 (L1 – L4), each level is interconnected with each other, and higher order levels subsume lower ones. Therefore, one could not gain *L2* without acquiring *L1*, and hence SA levels are cumulative and subsuming. For example, *L2* assumes *L1* is in place, and *L3* assumes both *L2* and *L1* are in place etc. For instance, one could not analyse event logs generated by Endpoints if they had not produced the logs in the first place. Similarly, one could not tell if sensory information is incorrect or incomplete if sensor signals could not be tracked or received in the first instance. Further, projection of the current and future situation is impossible if there is no awareness of the current situation in the first instance. In addition, resolution is impossible if there is no subsequent analysis of the current situation in order to understand what could have caused it. In summary, all of the SA levels are interlinked and interwoven, and most importantly, concentric and subsuming.

1) *Perception* (Level 1): Perception is the first level in a situation awareness application. At this level of Cyber SA, security analysts are knowledgeable of the elements in the network and are able to gather raw piece of evidence of situations perceived in the network, such as alerts reported by intrusion detection systems, firewalls, scanners as well as the time these pieces of security evidence occurred, and the specific control (source) that reported the alerts or generated the logs. This involves the use of individual and independent toolkits to monitor the network. Whilst these individual and independent toolkits (point solutions) gather raw data about perceived situations, and hence offer a level of protection to computer networks of cyber-attacks; unfortunately, each point solution is directed toward detecting a specific type of situation. Hence, detection of widespread or enterprise-wide situations is still challenging (Onwubiko, 2008); more so, the way they are deployed, usually localised, makes it extremely difficult to assess enterprise-wide situations, or quantify associated interdependent risks accurately and swiftly. At the *perception* level, information about the status, attributes and dynamics of the relevant elements in the environment may be known; and it is also possible to extend the classification of information into meaningful representations that offer the basis for comprehension, projection and resolution (Salerno et al., 2004). As shown in Figure 2, we argue that unless perception exists, then there is no basis for comprehension let alone higher SA levels, such as projection and resolution.

2) *Comprehension* (Level 2): At this level of situation awareness, the security analyst uses a number of tools, techniques, methodologies, processes to aggregate, analyse, synthesise and correlate pieces of evidence perceived in the network and from external sources to gain higher degrees of meaningfulness and understanding than those acquired at *L1*. *Comprehension* involves a determination of the relevance of the evidence captured to the underlying goal of resolution of the situation (Salerno et al., 2004). Hence, comprehension offers an organised picture of the current situation by determining the significance of the evidence perceived together with the importance of the assets being monitored. Further, it is pertinent to note that when new set of evidence becomes available the knowledge-base is updated to reflect this change.

3) *Projection* (Level 3): At this level of situation awareness, security analysts now possess the capability to make accurate future prediction or forecast based on the knowledge extracted from the dynamics of the network elements, leveraging on *L2*. The analyst's ability to make accurate future forecast can be enhanced by the use of powerful monitoring systems and technologies that are able to detect, deduce and predict patterns of occurrence of future events. For example, early warning systems are able to make forecast of future occurrences of weather situations. The use of systems with this capability in Cyber would certainly enhance operator SA, and enable better planning and the use of preventative controls to address potential situations. *Projection* answers the questions, what cyber situations are possible, what possible ways can current situations be exploited further or escalated, and what potential controls may be needed?

4) *Resolution* (Level 4): At this level of situational awareness, security analysts are able to recommend and implement adequate countermeasure controls required to treat risks inherent or interdependent in networks. *Resolution* as part of the core SA was first discussed in situation awareness by (McGuinness & Foy, 2000), as an extension of Endsley's SA levels. It is about the necessary actions required to address network situations when they occur.

4 CYBER SA APPLICATIONS

We propose a Cyber SA Instantiation Model, an overlay of the Endsley's modified process model, as shown in Figure 3. This instantiation model allows Cyber SA applications to be developed consistently. Further, since it is an overlay model, it enables situation awareness process model to be contextualized and referenced when building new Cyber SA applications, or assessing existing Cyber SA applications.

The aim is to provide a building block that underpins a foundation that allows SA to be understood consistently across various domains in Cyber.

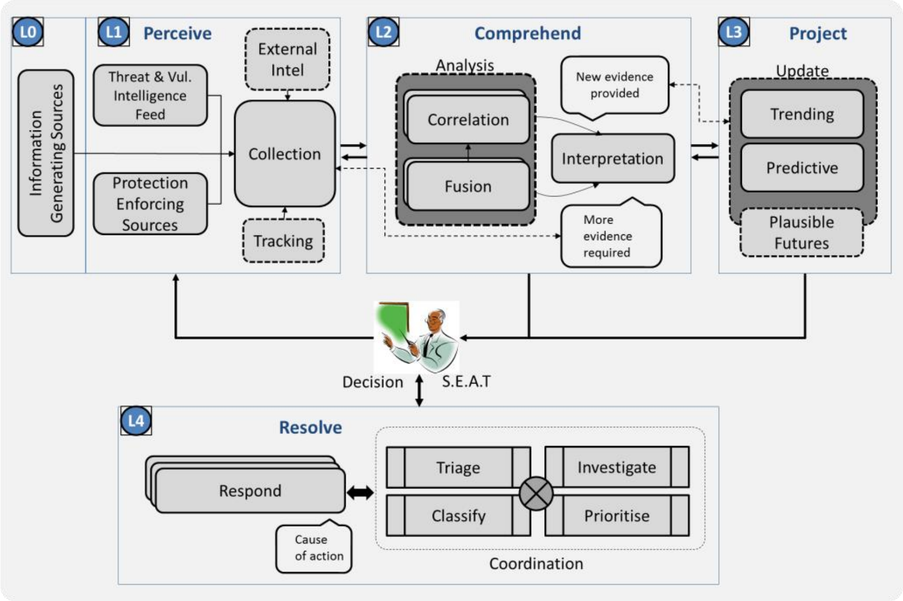

FIGURE 3: CYBER SA INSTANTIATION MODEL

The Cyber SA instantiation model (see Figure 3) overlays Endsley's modified model and are described as follows. The terms used in this model are generic so that the model is relevant and applicable across the Cyber domain.

There are five broad sources of awareness in this model. The first is classified as *information generating sources*. These are Log Sources[1] that are targets of an attack, compromise or exploitation, and by their very

[1] A Log Source is a basic piece of computing device that generates event logs as a result of object activity or interaction; they can be physical or virtual instantiation of a system or a subsystem.

nature, are unable to detect an attack unless through other mechanisms inbuilt into them. For example, your smartphone, laptop, desktop, server, document folders, shared drives etc. They are regarded as *information generating sources* because they produce or generate event logs when an activity or interaction happens. The event logs the generate may contain pieces of evidence symptomatic of an attack; further, without the generated event logs, which could be analysed to detect if and when they have been compromised, then an attack could happen and still go unnoticed. So any object capable of generating logs or transactional information is regarded as an information generating source in the broadest sense, and are classified as *L0*.

> Note: *L0* systems or subsystems may have in-built or/and installed protection enforcing mechanisms such as sensors like anti-virus software, host-based intrusion detection systems, etc. So it is important that *information generating sources* are classified separately from any other protection enforcing mechanisms they may have installed or in-built in them.

There are four distinct categories of *L1* awareness sources as shown in Figure 3 as follows:

Protection enforcing sources – These are systems or subsystems that enforce security policy or protection in the network, i.e. firewalls, IDS, sensors, antivirus servers, anti-DDoS etc. While the generate logs of their own, they also capture logs of the state of the network segment they monitor, and hence are classified differently.

Vulnerability and threat intelligence gathering sources – These are intelligence feeds which could come from the networks being monitored or from external sources. For instance, CERT announcements, vendor vulnerability intelligence, threat information etc. The offer enrichment of the already existing awareness and hence complement a current SA ‘picture’ to enable improved comprehension.

Tracking – provides essential information of external transient threats for instance, geographic information systems (GIS), radar, geolocation etc. As shown in figure 3, intelligence gained through tracking are transient and occurs when intelligence of both internal and external threat actors and sources are perceived and hence monitored.

External Intel – refers to all the external sources of intelligence. External intelligence can be gained through mechanisms such as social media intelligence, government intelligence, agency intelligence, CERT intelligence etc. some of which are ‘wetware’, that is, human based intelligence in addition to voice and data related intelligence. It is the type of awareness which can be gained using OSINT (Open Source Intelligence). An example of external intelligence includes the use of social media data to deduce or infer future attack or unrest. For instance, social media analysis has been used to detect future unrest (Compton R., De Silva, L., & Macy, M., 2013). Government agencies are another source of external intelligence. They are likely to know when an attack, Cyber or not, may be about to happen, and how this may be conducted may not be fully known, but bringing this intelligence to bear in Cyber may mean that cross correlation of various intelligence source will need to be conducted in order to gain better comprehension of the situation.

Collection is the central mechanism that allows these disparate pieces of evidence to be collected, gathered and made available to the *L2* mechanisms for analysis. It is important to note that some of the technologies mentioned in *L1* can be argued to perform some *L2* capability to a degree. Take firewalls for instance, some web application firewalls (WAFs) and Layer 4 firewalls may be argued to perform a degree of localized comprehension, i.e. an understanding of a ‘minimalistic picture’ of issues happening in the segment of the network they are deployed. In this paper, though, we are not focusing on arguing which technologies where or not, the focus is understand that these technologies can perform multiple functions, and therefore, may belong to different categories of the SA levels regardless. Unlike Tadda & Salerno (2009), we argue that not all sources are *L0*. Certainly, there is a degree of perception obtained from *protection enforcing sources* that make them able to detect situations in the network, for example, protection enforcing sources, such as firewalls or AVs are able to detect malware, understand traffic payload information, malicious or otherwise, perform traffic prioritization, filtering and inspection. Therefore we believe that they provide valuable cues to the operators that enable awareness of situations, hence are categorised as *L1*. There is a vast difference between *awareness* and *understanding*. Understanding involves so much more than awareness, and the capability to do so may be beyond certain systems, mechanisms or entities.

Intelligence gathered in *L1* are analysed in *L2* to understand fully the situation, determine impact, associated risks, cause of action and possible mitigations. To achieve this, intelligence collected from the various sources in *L0* and *L1* must be fused (combined) and correlated. Doing this offers the operator an enhanced situation awareness, better comprehension and understanding over those of individual, single and silo or localized sources in *L0* and *L1*.

Comprehension (L2) – comprises of analysis tools and techniques to better understand situations that occur in Cyber. It is pertinent to not that analysis is not a one-off activity, rather a continuous, real-time process that incorporates technology to perform automated, swift and repetitive tasks aimed at providing actionable recommendations on what can be done to address the current or impending future situations. Since intelligence can often appear conflicting between or among sources, and also because often times, intelligence can be incomplete or contradictory, therefore analysis techniques must be such that they can make meaningful "reasoning" of the situation, especially when intelligence are missing, incomplete, contradicting or conflicting. For example, imagine a hypothetical case, where a rogue sensor was able to join a network, and hence able to send its information to the central collection area. Information provided by this sensor are likely to skew information produced by the other reliable sensors, therefore analysis techniques are required that are able to deal with situations like this.

Further, the model advocates for the fusion of intelligence so that better understanding of the situation can be gained. *Fusion* allows disparate and somewhat unrelated events or activities to be combined in order to understand the 'bigger' picture. *Correlation* allows intelligence from many sources to be analysed in order to interplay and link evidence from across many source to understand their relationships.

Finally, analysis is meaningless if its outcome cannot be interpreted and well understood. At a coarse level the basic building blocks to allow for comprehension to happen are shown in the model, and they can be instantiated through the use of many tools and techniques. The model is not prescribing specific tools or technologies to use; rather, its focus is on the "*what"* rather than the "*how*".

Projection (L3) – is reliant on comprehension. This means "analysed intelligence" can be used to predict future states or situations. More so, this should be a real-time continuous process that allows the situation 'picture' to be updated when new and current intelligence becomes available. Projection allows the current situation to be monitored in order to track when the current situation changes so as to update the overall picture, and hence recommend possible mitigations or mitigation approach.

Resolution (L4) – is focus on what needs to be done in order to remedy, recover and resolve situations or respond to future situations observed through security monitoring, threat intelligence, tracking and external intelligence. The goal here is to triage, classify, prioritise and investigate

Cyber situations in order to resolve, remedy and recover. This requires the coordination of a number of specific functions, which on their own require specialist applications, skills, experience and expertise. This is why Cyber SA, like all SA applications, is a multidisciplinary and interdisciplinary domain.

In summary, the proposed instantiation model allows situation awareness to be instantiated, implemented or assessed across the Cyber domain. The model can be used in Security Monitoring, CERT, Computer Network Defence (CND), Active Cyber Defence (ACD) etc. As a model, it allows for low level processes to be defined, developed and applied according to specific organisational needs underpinned by strategy, risk appetite and risk tolerance.

5 MISCONCEPTIONS

There are a number of misconceptions with Cyber SA, here are some notable ones.

1. Some vendors are selling threat intelligence reports as Cyber SA. Threat and vulnerability feed is only one source of intelligence to a truly Cyber SA application (see Figure 3). Likewise, threat and vulnerability intelligence report is only an output from a Cyber SA application; unfortunately, intelligence report alone is not Cyber SA but an outcome.
2. Data Collection, Big Data or any repository that stores historic and current data sets is not Cyber SA. While events or pieces of evidence of security monitoring can be useful in understanding situations, and so is big data, but collection is not SA, but only one aspect of an attempt to present any ‘organised picture’ from which analysis can take place (see Figure 3).
3. Data Sharing or Intelligence Sharing is not Cyber SA. While intelligence sharing will help enrich the ‘overall picture’ and aid better understanding of perceived or impending situation, it is still only one aspect, and a single source of Cyber SA intelligence.

6 CONCLUSION

Cyber SA is a multidisciplinary and interdisciplinary domain. It is no different to the application of SA to other domains, such as SA in ATC, Medicine and Transportation. While that is the case though, Cyber SA is an emerging discipline; hence the area is yet immature, embryonic and not fully developed. Like any new area, there are not much building blocks, processes, standards and policies to enable this to be well developed. This has led to some confusion with definition of key terms, the application of the concept to Cyber, and in general an incoherent use of terms.

With every new innovation or its application, there is potential for misconceptions, misinterpretation and downright misunderstanding. This has led to situations where very many ‘things’ have now been ‘branded’ Cyber SA, many of which have nothing to do with situation awareness. So in this chapter, we have therefore introduced Cyber SA, provided definitions, examples and discussed applications of situation awareness in the Cyber domain. We proposed a Cyber SA instantiation model, and showed how this model can be used to assess or enable the application of SA in the Cyber domain.

Also, the chapter discussed what Cyber SA is, and what it is not; addressing some notable misconceptions in the discipline.

All the different levels of situation awareness were explained in this chapter with examples showing what each specific component does and should focus on. Further, how SA can be applied in Cyber security and security monitoring are discussed.

6.1 Future Work

Future work should focus on standardisation of the Cyber SA discipline by providing building blocks, policies, processes, assessment and measurement criteria for Cyber SA application to be developed or assessed.

Further, new Cyber SA application should focus on building applications that are situation-aware, and considers requirements criteria, functional and non-functional as have been discussed by previous contributions (Onwubiko, 2009, Onwubiko, 2011b).

6 REFERENCES

Bidou, R., 2002. Security Operation Centre Concepts & Implementation. Retrieved 18th September 2016 from http://iv2-technologies.com/SOCConceptAndImplementation.pdf

Compton R., De Silva, L., & Macy, M., 201. Detecting future social unrest in unprocessed Twitter data: “Emerging phenomena and big data”. IEEE International Conference on Intelligence and Security Informatics (ISI), 2013, DOI: 10.1109/ISI.2013.6578786

Cumiford L. D., (2006). Situation Awareness for Cyber Defense, 2006 CCRTS – The State of the Art and the State of the Practice, Sandia National Laboratories, MS 0455, USA, 2006.

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.

Endsley M. R. and Garland D. J., (2000). Situation Awareness Analysis and Measurement. CRC Press, FL, USA, 2000.

Google Search (2016). Cyber Situation Awareness. Google search of the "Cyber situation awareness". Retrieved 13th September 2016 from https://www.google.co.uk/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=cyber+situation+Awareness

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.

Eiza, M. h., Owens, T. and Ni, Q. (2016). Secure and Robust Multi-Constrained QoS Aware Routing Algorithm for VANETs in *IEEE Transactions on Dependable and Secure Computing, Vol.13, 2016 1st Trimester Issue Jan-April, 2016*

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

Onwubiko C., (2008). Security Framework for Attack Detection in Computer Networks. VDM Verlag Publisher, 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. (2011a). 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*.

Onwubiko, C. & Owens T.J. (2011). Review of Situational Awareness for Computer Network Defense. In C. Onwubiko and T.J. Owens (Eds.) *Situational Awareness in Computer Network Defense: Principles, Methods and Applications*.

Onwubiko, C. (2015). Cyber Science 2015 – International Conference on Cyber Situational Awareness, C-MRiC.ORG, London, UK ISBN 978-0-9932338-0-7

Onwubiko, C. (2015a). The Role of Situational Awareness in Cyber Security and Cyber Defense Strategy. In C. Onwubiko (Ed) Cyber Science 2015 – International Conference on Cyber Situational Awareness, C-MRiC.ORG, London, UK ISBN 978-0-9932338-0-7

Onwubiko, C. (2016). Cyber Science 2016 – Pioneering Research & Innovation in Cyber Situational Awareness, C-MRiC.ORG, London, UK ISBN 978-0-9932338-1-4

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.

BIOGRAPHICAL NOTES

Dr Cyril Onwubiko is Director, Cyber Security and Information Assurance (IA) at Research Series Limited, where he is responsible for directing strategy, IA governance and cyber security. Prior to Research Series, he had worked in the Financial Services, Telecommunication, Health & Government and Public services Sectors. He is experienced in Cyber Security, Security Information and Event Management, Data Fusion, Intrusion Detection Systems and Computer Network Security; and vastly knowledgeable in Information Assurance, Risk Assessment & Management.

Cyril holds a PhD in Computer Network Security from Kingston University, London, UK; MSc in Internet Engineering, from University of East London, London, UK, and BSc, first class honours, in Computer Science & Mathematics.

Cyril has authored several books including "*Security Framework for Attack Detection in Computer Networks*" and "*Concepts in Numerical Methods*", and edited books such as "*Situational Awareness in Computer Network Defense: Principles, Methods & Applications*", and *Cyber Science 2016* & *Cyber Science 2015 – International Conference on Cyber Situational Awareness, Data Analytics and Assessment*. He has over 30 articles published in leading and most prestigious academic journals and conferences.

Reference to this paper should be made as follows: Onwubiko, C. (2016). Understanding Cyber Situation Awareness. *International Journal on Cyber Situational Awareness*, Vol. 1, No. 1, pp11-30.