# Designing Information Systems and Network Components for Situational Awareness

**Cyril Onwubiko**
*Intelligence and Security Assurance, Research Series Limited, United Kingdom*

## ABSTRACT
Operators need situational awareness (SA) of their organisation's computer networks and information systems in order to identify threats, estimate impact of attacks, evaluate risks, understand situations and make sound decisions swiftly and accurately on what to protect against, and how to address incidents that may impact valued assets. Enterprise computer networks are often huge and complex, spanning across several WANs and supporting a number of distributed services. Understanding situations in such dynamic and complex networks is going to be time-consuming and challenging. Operators SA are enhanced through a number of ways, one of which is through the use of situation-aware systems and technology. Designing situation-aware systems for computer network defence (CND) is difficult without understanding basic situational awareness design requirements of network applications and systems. Thus, this chapter investigates pertinent features that are foundation, essential and beneficial for designing situation-aware systems, software and network applications for CND.

## INTRODUCTION
In the last fifteen years the application of situational awareness has been revolutionary, particularly in Air Traffic Control (ATC), and Defence and Military operation where SA has been extensively researched. ATC operation, for instance, can be compared to CND operation; unfortunately, while the application of situational awareness to computer network defence is still in its embryonic stage, its application to ATC is mainstream (Onwubiko C., 2009).

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, intrusions, disruptions or other perceived unauthorised actions that could compromise or impact defence information systems and networks. CND is achieved through a collective effort by personnel who monitor, manage and maintain defence systems, networks and infrastructures, such as network operators, security analysts, systems administrators and network engineers. This group of personnel are referred to, in this chapter, as operators, ('human' operators). 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.

Cyber-attacks to computer networks are growing and evolving. For example, code-driven attacks, deliberate malicious software attacks, espionage, distributed denial of service attacks, phishing and the recent computer electronics attacks (E.g. Stuxnet). All these contribute in demonstrating the complexity and challenges faced in a CND environment.

Situational awareness is the process of perceiving the elements in the environment, understanding the elements in the environment, and the projection of their status into the near future (Endsley M. R., 2000). SA underscores situation assessment in order to make accurate forecast in dynamic and complex environments. 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 C., 2009). Hence, we believe that the application of SA in CND will yield unprecedented benefits akin to SA for safety and security in aircraft, flight operation and safety controls.

In this chapter we investigate task and system requirements that support situational awareness in CND. Task requirements are human operator-specific tasks such as risk assessment, protective monitoring and decision making. System requirements are automated system-specific tasks completed by computer systems and network appliances. The elicitation of task and system requirements for CND is the foundation for building CND systems and applications that are situation-aware; and the use of situation-aware systems and applications in a CND environment certainly enhances operator situational awareness.

Situational awareness as a human mental process is enhanced by the use of technology to access, analyse, and present information to have greater understanding of existing situations and how they may change over time (ESRI, 2008). Thus, the aim of this chapter is to investigate situational awareness in computer network security, and to evaluate task and system design requirements (functional and non-functional) that CND systems should possess to enhance operator situational awareness. According to Endsley M. R., and Garland D. J., (2000), the enhancement of operator situation awareness has become a major design goal for those developing operator interfaces, automation concepts and training programs in a wide variety of fields, such as, air traffic control, power plants and advanced manufacturing systems. It is equally important to extend this design assessment to CND infrastructure, systems and applications.

The remainder of this chapter is organised as follows. Section 0 describes situational awareness in network security. Section 0 discusses our design requirements framework for developing situation-aware CND systems and applications. Design requirements discussed comprises both functional and non-functional requirements. Section **Error! Reference ource not found.** elaborates on our contribution, and outlines benefits of the work, which strengthens the usefulness of the contribution. Finally, the chapter is concluded in section 0.

## NETWORK SECURITY SITUATIONAL AWARENESS

Situational awareness is described as knowing what is going on around you and within that knowledge of your surroundings, knowing what is important (D'Amico A., and Kocka M., 2005). Situational awareness stems from human factor and cognitive studies. It has been well-studied and applied to several disciplines, including psychology, aviation and military operations, since the seminal work of Endsley M., (1995). SA involves both a person with his

cognitive processes, as well as a situation with several information types and statuses (Lambert D. A., et al, 2004). SA is very complex and involves very dynamic states. For example, computer networks with hundreds of network objects (firewalls, IDSes, routers, switches, servers, PADs), maintaining a consistently high situational awareness over these objects can be challenging. The operator through his mental models, experience and training, tries to monitor the network, using a number of mechanisms, technologies and toolkits, each device having a perception of the network being monitored.

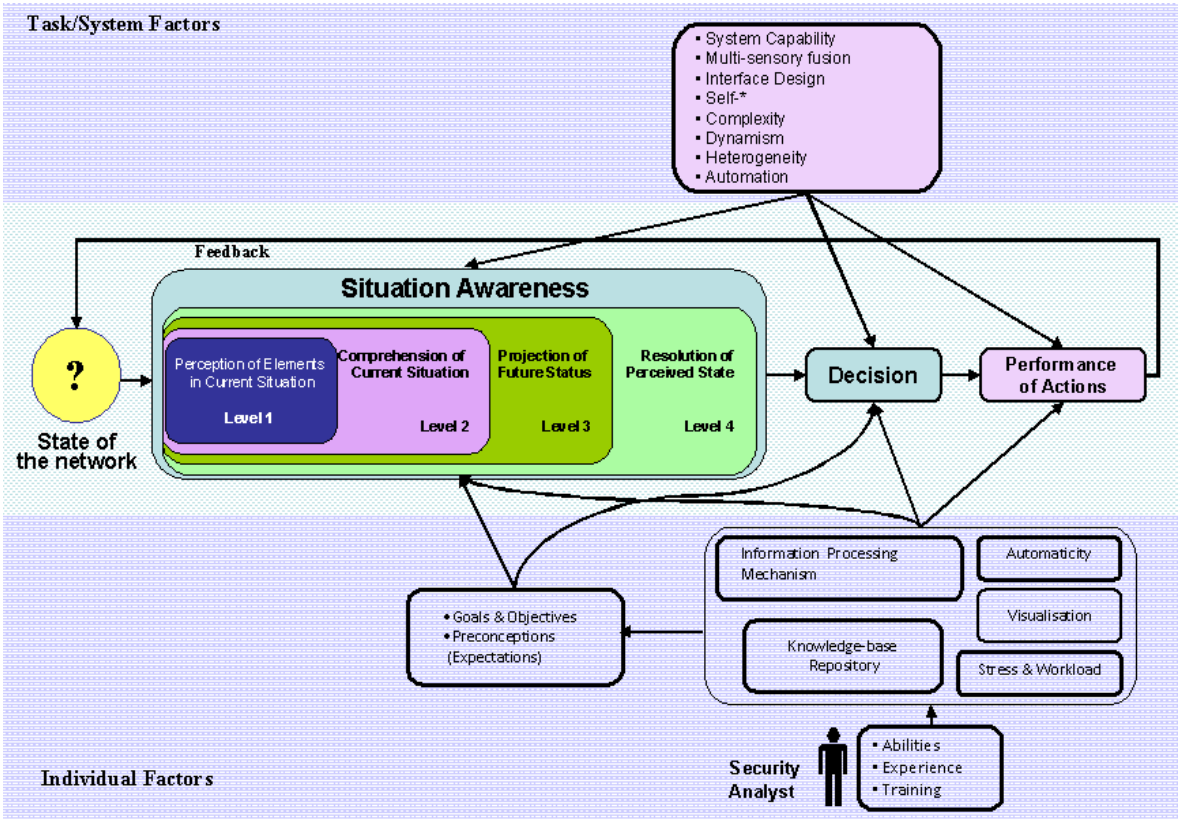


**Figure 1: Network Security Situation Awareness Model**

Figure 1 is adapted from Endsley's situation awareness reference model (Endsley M., 1995), which presents three levels of situation awareness, *perception*, *comprehension* and *projection*. In addition to McGuinness and Foy's (McGuinness B., and Foy L., 2000) extension of Endsley's SA model that includes *resolution* as the level four situation awareness component.

These terms (*perception*, *comprehension*, *projection* and *resolution*) are discussed in this chapter in relation to network security situational awareness. Thus, *perception* deals with evidence gathering of network situations, *comprehension* deals with the analysis of the set of network situation evidence, and also involves with the deduction of exact threat level, identification of attack types, and understanding of associated or interdependent risks. *Projection* deals with predictive measures to address future incidents, while, *resolution* deals with controls to repair, recover and resolve network situations.

To achieve some degree of situational awareness, as shown in Figure 1, we need both Task and systems factors, and individual factors. Task and system factors are system-specific tasks and systems requirements that assist individuals/operators gain situation awareness. For example, systems capability, automation and interface design. Individual factors are human-

factor attributes that could enhance or impact operator situational awareness, such as training and experience, or stress and workload. While task and systems factor requirements are discussed in section 0 of this chapter, individual factors are not within the scope of this contribution. This chapter focuses on task and system factor requirements that are essential in designing situation-aware systems and tasks for CND.

*Perception, comprehension, projection* and *resolution* are core SA components, and each is discussed in details in relation to computer network security, as follows:

1) *Perception* (Level 1): At this level of situational awareness, 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, firewall logs, scan reports, 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 from cyber-attacks; unfortunately, each point solution is directed toward addressing a specific attack. Hence, detection of widespread or enterprise-wide attack situations is still challenging (Onwubiko C., 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 are known; and it is also possible to extend the classification of information into meaningful representations that offers the underlying for comprehension, projection and resolution (Salerno et al., 2004).

2) *Comprehension* (Level 2): At this level of situational awareness, the security analyst uses techniques, methodologies, processes and procedures to analyse, synthesise, correlate and aggregate pieces of evidence data perceived in the network from network elements to gain higher degrees of meaningfulness and understanding than those acquired at Level 1 SA. *Comprehension* also 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. And when new set of evidence becomes available the knowledge-base is updated to reflect this change.

3) *Projection* (Level 3): At this level of situational 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 SA. 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 CND environment would certainly enhance operator SA, and enable better planning and the use of preventative controls to address potential situations. *Projection* answers the questions, what network attack are possible and what 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 B., and Foy L., (2000), as an extension of Endsley's SA levels. It is about the necessary actions required to address network situations when they occur.

In many respects, SA is comparable to the OODA (observe, orient, deduce and act) loop. The OODA decision control was first proposed by Boyd J. (1987) used in Command and Control (C2). 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, interface, Human Computer Interface (HCI) interactions and all the other requirements mentioned (see Section 0), to enhance situational awareness of the network being monitored, and then decide the best cause of action to be taken.

Whether SA or OODA, the approach for CND are:

- 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 analyse data from a number of distributed sensors deployed in and around the network;
- Fourth, reliant on operators' mental models (past knowledge of network behaviours, experience and training), they are able to make projections about future network states. For example, due to observed network traffic and volumetric, an experienced operator could make accurate estimation of when the network is under attack from evolving computer worm mutant or variants of a self-propagating malicious code.

## DESIGN REQUIREMENTS FRAMEWORK FOR SITUATIONAL AWARENESS IN CND

In this section, task and system design requirements that enable operator situational awareness in computer networks, information security and CND are investigated.

Eliciting and capturing the requirements of a system or an application is one of the first fundamental steps in software and systems engineering. Since designing and implementing an

extensible system is complex, as is the case with designing situation-aware systems, we need to clearly establish the requirements, which can be either functional or non-functional.

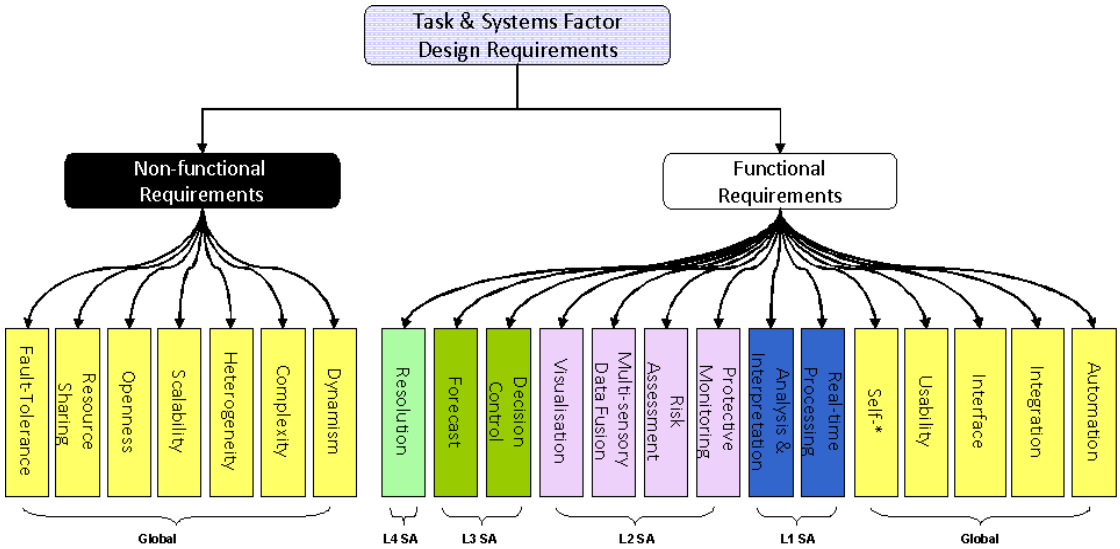


*Figure 2: Task and System Factor Situational Awareness Design Requirements*

Figure 2 is our proposed task and system factor design requirements framework for computer network defence. It consists of two main categories, functional and non-functional requirements. Further, requirement attributes are further partitioned in accordance with core SA component requirements, such as global, L1 SA, L2 SA, L3 SA and L4 SA. *Global requirements* are requirements performed by the system regardless whether they are functional, non-functional, or pertaining to a particular SA level. *L1 SA* are level 1 situational awareness specific requirements. *L2 SA* are level 2 situational awareness specific requirements. *L3 SA* are level 3 situational awareness specific requirements; finally, *L4 SA* is level 4 situational awareness specific requirement.

Functional requirements are concerned with the functions that the system can perform for its users (Emmerich W., 2000). Functional requirements, therefore, are usually localised in the system, and with particular components of the system. For example, human computer interface (HCI) is localised in the systems' interface component, while real-time processing is localised in the memory and processing engine of the system.

Non-functional requirements are concerned with the quality of the system. They are usually difficult to be attributed to any particular component of the system or sub-systems of the system. They are, rather, global system qualities; hence non-functional requirements typically have serious impact on the overall architecture of the chosen system. For example, a distributed system may have serious performance impact if it is not scalable or robust, whereas this for a centralised system does not apply, hence scalability as a non-functional requirement will have an impact on the overall architecture of the system (whether distributed or centralised).

## FUNCTIONAL DESIGN REQUIREMENTS FOR SITUATIONAL AWARENESS IN CND

Situation awareness attributes are discussed in relation to functional characteristics of SA in computer network security (CNS) and computer network defence (CND). This list is by no means exhaustive, however, the necessary steps toward understanding the essential attribute to designing and implementing SA in computer network security have been strategically presented, as follows:

1. Automation,
2. Integration,
3. Interface,
4. Usability,
5. Self-*,
6. Real-time processing,
7. Analysis and interpretation,
8. Protective monitoring,
9. Risk Assessment,
10. Multi-sensory data fusion,
11. Visualisation,
12. Decision control,
13. Forecast,
14. Resolution.

### AUTOMATION

Human factor researchers in the early 90s believed that automation of *cognitive-aware* systems (systems that performed cognitive tasks) contributed to errors and failures in SA, and often, were metaphors to performance degradation in SA (Wickens C. D., 1992; Endsley M. R., 1996). One would understand their standpoint, especially given the time period when these debates occurred. Their major concern was roles were swapped between *humans* and *machines*. In the past, *humans* performed tasks, but recently, machines are now automated to perform these tasks, while humans now monitor over automated systems.

The advent of very powerful computing systems and the possibility of real-time processing have made automation of technologically-enabled and situation-aware tasks more attractive, appealing and ubiquitous. This is a paradigm shift in the 21st century. The desire to automate every task, (such as, physical, logical, perceptual, and even cognitive) has increased. Furthermore, it is widely believed that automated systems perform better than humans in

solving most real world problems, especially those requiring speed, accuracy and reliability. Arguable as it may be, current trends show that automated systems are preferred over humans in performing rigorous numerical, medical and physical tasks. However, automation of cognitive tasks may be different. While the mental models (residual knowledge, experience and training) of the operator are essential to understanding situations in the network, there is certainly a genuine need for operators to leverage on technology and system automation to gain and enhance operator SA. Automating the integration, processing and analysis provided by these systems should go a long way in helping operators gain short term SA over these network probes. Automation of technology is certainly a requirement when designing situation-aware systems and application for CND.

## INTEGRATION

Computer systems and their components must interact either as autonomous, dependent or interdependent systems. To enable this relationship, computer system components are integrated, often tightly coupled, so that they can interoperate as a self-interacting autonomous system. Using a computer system, for example, separate pieces of components, such as monitor, keyboard, mouse, memory, processor, and storage media are collectively integrated into a single autonomous system referred to as a computer system. Similarly, a network comprising a hub, server and workstation is a collection of autonomous and interdependent systems that collaborate to enable communication. It is pertinent to mention that the possibility to integrate system and system components, a class of powerful systems has evolved, such as the cyber-physical systems (CPS).

Cyber-Physical Systems are embedded systems that integrate computation with physical processes. These class of systems, usually, have embedded computers and network monitors that control the physical processes, and often with feedback loops where physical processes affect computations and vice versa (Lee E. A., 2006). Examples of CPS systems, include communications systems, distributed robotics, defence systems, manufacturing and smart structures. The ability for this class of new systems to provide the much needed collaborative framework provides operators the opportunity to make timely savings on processing, analysis and remediation by leveraging on the capabilities of these to provide real-time or near real-time responses to perceived attack. While CPS systems in themselves are not a requirement for CND, however, integration provides the platform to create multi-functioning systems that assist operators in analysing network probes, events and alerts, which consequently, enable operator gain enhanced SA of the network. Systems integration and application integration are foundation requirements in CND whether it is for the purposes of situational awareness or not.

## INTERFACE

Today's information and communications technology (ICT) systems are complex. These systems use a plethora of technologies and software to implement complex business logics, some of which involve a finite number of background processes that are transparent to the operator, and therefore make it challenging for the operator to swiftly identify sequence of erroneous actions or detect fault in the system or spot when an abnormal situation is happening. To assist operators to detect, diagnose and remedy abnormal situations swiftly,

complex computer systems should provide interfaces that enable human computer interaction. Operator situational awareness will be enhanced if systems can provide interactive interfaces that enable human interaction, such as graphical user interfaces (GUI), ASCII interface, command line interface, and command and control interface. These interfaces can be used for human computer interaction to enable feedback loop control. Whatever the interface (GUI or command line), systems and system components need to interact (intra and inter communications), integrate and interoperate either as autonomous or interdependent systems. This is one of the reasons why interface design has been acknowledged as a significant factor when assessing SA in systems. Thus, according to Endsley M., and Garland D. J., (2000), one of the primary reasons for measuring SA has been for the purpose of evaluating new system and interface designs.

Human computer interface designs do affect operator performance and system safety. According to Sandom C., (1999), the design of HCI can have a profound effect on safety assurance, particularly during emergency situations. For example, when emergencies arise and system operators must react swiftly and accurately, the situational awareness of the operator is critical to their ability to make decisions, revise plans and to act purposefully to correct the abnormal situation. This sentiment emphasises the importance of designing HCIs to support situational awareness, especially in complex and dynamically changing environment such as in network monitoring and computer network defence.

We believe that the quality of the interfaces a system offers determines the degree of human interaction possible. Hence, SA designers for CND should ensure that modern network systems are capable of offering a variety of HCI interfaces that aid human interaction.

## USABILITY

Usability (user friendliness) is a design and development construct for testing a system's functionality and how the system interacts with its users. Usability development practices offer a means of quantifying, designing and testing the applicability or fitness of a system. According to Borja A. T. (2003), the application of usability engineering in the product's lifecycle reduces cost over the life of the product's development, by reducing the need to add missed or fix unusable functionality later in the development cycle. Systems that are intuitively easy to use are preferable for operators who are faced with many changes and the complexity of dynamic network activities. So designer should ensure that systems are tested for usability and the use of system to perform work should of minimum easy, that is, it should not require steep learning curve in order to intuitively work out how a system should be used. The difficulty to use system can impose unnecessary constraint and add to the lack of situation awareness by adding to the workload of the operators. It is important that in addition to designing systems that offer the operator with the required information and capabilities, we also ensure that it is provided in a way that is useable cognitively as well as physically (Endsley M. R., 2000; Onwubiko C., 2009).

## SELF-*

Self-* is the collection of self-oriented attributes such as self-awareness, self-healing, self-reconfiguration, self-autonomous, self-discovery, self-analysis and self-defending that a

system performs by itself without human assistance. This list is not exhaustive, but the emphases is that self-* is systems requirements that CND systems could be evaluated against. Whether CND systems should possess self-* is open for discussion, and if asked, modern CND systems should possess a level of self-* attributes, provided it does not replace human intelligence and override human decision control, but should work together synergistically to offer better situational awareness to the operator. The operator will benefits, and invariably gain better awareness of the situation if the system possess a level of self-*, such that they could report internal and on-going situations to the operator, who through the gathering of other external information gain enhanced and complementary SA through the other cues available to them. For example, if a computer system has self-* capabilities to report that its processor cycle is consistently high over a period of time, and that the reason why the cycle is high is because of a new program the user had installed, and that this new program has a register conflict with another software running in background mode. And if the system can report to the operator, without much analysis by the operator, then, the operator would have enough cues to understand better the situation, and therefore, without such reports be able to decide (decision making) on an efficient cause of action, in time and accurately. If every component in the network possesses this level of self-* qualities, then maintaining consistently enhanced situational awareness of the network can be achievable. If this were to be possible, it will become the underpinning of self-* contribution in computer network defence; and presumably, useful to other areas life such as medical science, military operations and aviation.

## REAL-TIME PROCESSING

In computer network security, as with military defence, aviation and ATC, real-time processing of information, particularly, suspicious traffic, military intelligence or intelligence regarding enemy presence is required. To achieve a higher level of situation awareness, the capability of the computing device used for SA analysis must possess the ability to provide real-time processing of data and information. This is analogous to a person's human cognitive being able to offer instant thoughts about a perceived situation. The absence of real-time processing hinders the possibility to provide swift and instant response to perceived attacks, such that the *'detect, analyse, decide* and *respond*' paradigm in defence becomes less attractive. This will certainly render the application of SA in CND inefficient. Computing systems and their underlying software used for SA to analyse situations must possess the capability to offer real-time processing, spontaneous feedback mechanisms, and real-time responses. Real-time processing is important design functionality for systems and applications, especially, when such systems and application will be used for CND operations. For example, Cisco ASA 5500 series of firewalls can process up to 12Gbps of real world multi-protocol traffic (Cisco System Inc., 2011), while Juniper's latest ISG 2000 integrated security gateways favour of intrusion detection and prevention systems (IDP) can process information at about 3Mbps (Junipers Networks, 2011). This goes to demonstrate the overwhelming importance of real-time or near real-time processing for CND systems and applications.

## ANALYSIS AND INTERPRETATION

Analysis provided by computer network monitoring systems should be such that it can provide system administrators and network operators a degree of situational awareness to

enable them identify and remedy dynamic network situations swiftly. Analysis must be built into networking devices such that a suite of multimedia channels can be utilised. For example, system (or system component) should be able to display alert information (visual), send alert information (as text, email or log messages) and provide audible alerts (alarms). The provision of a variety of alerting channels ensures that operators are provided with the required medium to enable them detect, identify and diagnose swiftly dynamic changes that occur in networks. These changes can be faults, errors, attacks or changes in traffic volumetric. When designing network systems and components for SA, designers should ensure that analysis components of systems are able to provide operators a variety of alerting and reporting channels to enable enhanced situational awareness. In ATC for instance, modern aircrafts are designed to provide both the ATC operators and pilots a variety of alert reporting channels. For example, the aircraft cockpit is designed to display weather information graphically, offer textual information of the same event, and also provide audible (audio) of the changes in the event being reported. For instance, when an aircraft changes altitude, whilst this is displayed on the computer display unit, both text and audio (sound) are provided to ensure that pilot crew are made aware of the changing situation. This has improved pilot's situational awareness as a result of information flow between the pilot and cockpit (Mulgund S., et al. 1997), and this would enhance better interpretation as multiple channels can be correlated.

Multimedia enhancement and support in the analysis is essential so that network warnings, errors faults and changes (situations) can be provided via audio, visual, textual, and pictorial (graphically). This is to ensure that network and security operators are presented with a variety of different channels and facets to enable them detect, diagnose, analyse and interpret dynamic network situations as them occur. Accurate interpretation of information and data is the key to achieving enhanced situational awareness and consequently making timely and accurate decisions. According to Endsley M. R., (2000), in the face of torrent of data, many operators may even be less informed. Hence information must be integrated and interpreted accurately for any operator to stand a chance of providing accurate and timely cause of action to an unknown situation. Situation-aware systems designers for CND operation should consider the provision of rich and wide-ranging analysis and interpretation modules/components for CND systems and applications.

## PROTECTIVE MONITORING

Protective monitoring is a task-specific level 2 SA that helps increase operators' situational awareness in computer network defence (see Figure 1). Protective monitoring is usually an operational task performed by human operators. It involves the use of technology to monitor networks and systems for on-going phenomenon in which data may be continuously changing. These dynamically changing situations are often times normal, and occasionally abnormal. Abnormal situations are suspicious situations that are processed with a view to addressing any situations such as errors, faults or attacks in the platform.

Protective monitoring as a CND requirement provides the provision for adequate accounting, logging and auditing of user and network activities of the platform, such that user interactions, actions and dynamic network activities are monitored, logged and analysed (real-time and retrospectively). User and network activities monitoring help security administrators to identify, detect and resolve abnormal network issues. Protective monitoring is usually

achieved through the use of a collection of several protective systems, such as firewalls, intrusion detection systems, identity management systems, log analysis and log integrity management systems to present to network administrators the network health, user interaction, traffic volume and abnormal activities which would be ordinarily impossible from either a sole administrator's or a single sensor perspective.

The benefit is an increased situational awareness of network administrators that offers overall status of the network health, which assists in the detection and identification of abnormal situations in the network or in systems within the network (Onwubiko, C., 2008). Protective monitoring is that aspect of CND that offers security analysts cues in the monitored network; provides the data (network traffic and log) that helps the analyst correlate, analyse and determine the level of perceived threat. And assembling these information, provides the analyst an understanding (comprehension) of perceived status of the network, and enable projection where possible.

## ASSESSMENT OF RISK AND INCIDENTS

Risk assessment in network security situation awareness is a level 2 SA, where perceived situations are assessed in order to identify on-going attacks, quantify states and estimate associated risks. Certainly, risk assessment is a very important step of the NSSA. Computer networks are under constant attacks. These attacks result from both attackers with malicious intents, and inadvertently from legitimate users of the system without malicious intents. Cyber-attacks, such as insider attacks, deliberate software attacks, espionage, phishing and denial of service attacks cause harm or predispose assets to harm leading to consequential loss to the organisation (Onwubiko C., 2008). Thus, the risks organisations face are real, evolving, serious and ever-changing, such that the need to adequately protect their critical and valued assets such as computer networks, computing infrastructures and systems can never be more timely.

## MULTI-SENSORY DATA FUSION

Multi-sensory data fusion (MSDF) is a task and system factor requirement, which is provided by the human operator through the use of technology. It is a process carried on multi-source data towards detection, association, correlation, estimation and aggregation (Onwubiko C., 2008). With MSDF data from multiple heterogeneous sources are combined to obtain better and higher degrees accuracy and richer inferences than those obtain from a single source. MSDF encompasses framework, theory, tools and techniques for exploiting the synergy in the data, information or evidence acquired from multiple sources, such as sensors, databases, intelligent sources and humans that helps us better understand a phenomenon and enhance intelligence (Hall D. L., and McMullen S. A. H., 2004).

Multi-source fusion is essential to network security situation awareness, particularly, level 2. It functions on the premise that evidence from multiple sources combined to detect attacks provides better understanding of attacks than a single source. According to Haines J., et al., 2003, "previous results indicate that no single control (for example, IDS) can detect all cyber-attacks. IDS research continues, but researchers have now turned their attention to higher-level correlation systems to gather and combine evidence from many heterogeneous intrusion

detection systems and to make use of this broader evidence base for better attack detection". A significant proposition with situation awareness in computer networks is that it enables security analysts in decision making, and consequently assist them to recommend efficient and adequate countermeasures to address observed situations, and also, to make prediction about future network states. In this respect, the provision of MSDF helps the analyst to identify on-going attacks in the network, comprehend network status and quantify associated risks.

It has been argued that the future of next generation cyberspace intrusion detection systems depends on the fusion of data from myriad heterogeneous distributed network agents to effectively create cyberspace situational awareness (Bass T., 2000). With cyberspace situational awareness network changes, deviation and variations can be easily perceived and analysed. This is beyond the capabilities of current intrusion detection systems. Hence the application of multi-source data fusion is essential to swiftly detecting enterprise-wide situations in computer networks (Onwubiko C., 2008).

Data fusion is a technique to aggregate sets of evidence regarding a perceived situation. The offering is that multi-sensory (multi source) data fusion is better in detecting wide spreading and enterprise-wide situations (network faults, threats and attacks) targeting most networks, and to achieve CND objectives, MSDF becomes pertinent. While MSDF implies the use of multiple sensors to gather and collect piece of evidence about situations perceived in the network, many modern network defence appliance are geared up to 'integrated' suite of products such as the unified threat management solution by Checkpoint, or the integrated security gateway suite by Juniper networks (Juniper Networks, 2011) and Cisco Systems Inc. (Cisco Systems, 2011). These products demonstrate the overwhelming need to design CND products that offer multi-sensory capabilities and support. The trend is also seen with open source products such as Snort IDS that provides the capability to combine several sensors such as Passive Operating System Fingerprint (P0F), Passive Asset Detection System (PADS), and TCP Tracker (TCPTRACK). Designing CND systems and application for SA is a significant contribution, and a factor to consider is ensuring that recent and modern systems and applications for CND can provide or support multi-sensor operation, integration and analysis.

## VISUALISATION

Patterns of attack or evidence gathered about security attacks need to be visualised to assist security analysts to swiftly spot, detect, decide and respond to attacks. This is also in line with the OODA framework. Security visualisation is the transfer of organised data and information into meaningful patterns or sequence to be visualised. It is part of the comprehension stage of the core situation awareness. Visualisation and user interface need to be selected based on their ability to provide elaborate representation of attacks perceived in the network. Visualisation allows network information to be displayed in such a way that it helps security analysts to detect patterns in traffic, and view large amount of information concisely. Hence, visualisation has proven to be a valuable tool for working more effectively with complex data and maintaining situational awareness in demanding operational domains (D'Amico A. and Kocka M., 2005).

Visualising network activities can be useful to both decision makers and security analysts in identifying patterns of attacks, and in decision making, control selection and cause of action. For example, visual analytics is essential to obtaining enhanced situational awareness in networks (Gregoire M. and Beaudoin L., 2005), understanding host-level netflow traffic in networks (Lakkaraju K., et al., 2004), and monitoring Internet security link-analysis (Yin X., et al., 2008).

There are significant efforts in developing CND visual analytic applications, for example, SIFT (Yurick W., 2005) and SILK (Carnegie Mellon, 2005), that are used to monitor network traffic and system status that assist operators gain better situational awareness of network activities.

## DECISION CONTROL

Decision making is an operator associated task that involves assessing the situation and then choosing an appropriate cause of action (CoA). According to (US FAA, 1991), decision making is a systematic approach to the mental process used by an operator to consistently determine the best possible course of action in response to a given set of circumstances. Situation assessment involves defining the problem and assessing the levels of risk associated with the situation and the amount of time required to solve the problem and the impact it may have if unresolved.

The fundamental underpinning of cognitive tasks in human factor is concerned with decision making of the various reasoning inputs. This is no different to situation awareness, say in computer network defence, medical operations, ATC, or military defence. All requires a great deal of decision making about a perceived and assessed situation. It requires decision about the level of threat perceived in the network, about the associated risks, it concerns decision about countermeasures required to adequately mitigate the perceived and assessed situation. Particularly in CND, for instance, networks are continuously being monitored and assessed for on-going suspicious traffic, suspicious behaviour or known fingerprints of attacks, and thereafter, decisions are made based on quantifiable risks estimated. Hence, situational awareness is essential for decision makers to efficiently manage their resources, and to greatly improve the rate and quality of human decision making (Gregoire M. and Beaudoin L., 2005).

## FORECAST

A truly situational awareness toolkit is able to make accurate predictions about future state. The goal of forecasting can be, either to find the likely future state assuming the present progression continues without intervention, or to determine a particular future state based on potential courses of action (D'Amico A. and Kocka M., 2005). To make accurate future predictions, current states and situations must be accurately assessed, evaluated and responded to. It is difficult to make correct prediction of future states if current situations and states cannot be determined satisfactorily. A forecast is often achieved by comparing baselines, or matching past to current states and situations, provided a reliable model of the system can be obtained. *Projection* provides awareness of how situations may develop over time by predicting or simulating possible scenarios, including the system's own actions and its dynamic effects (Lefebvre J. H., et al. 2005).

### RESOLUTION

Resolution of errors in system performance resulting from faults and failures in computer networks and systems infrastructures are important to correct anomalies, repair and restore systems. Errors, faults and failures affect the performance of computing systems and their offered services, such as integrity, confidentiality and availability. And without resolving these abnormalities in systems, their offered services will be rendered unusable, inefficient or unavailable. Resolution encompasses physical and logical restoration of computing infrastructures, network connectivity, and the dissemination of relevant battle-space situation information among cooperating analysts or operators.

## NON-FUNCTIONAL DESIGN REQUIREMENTS FOR SITUATIONAL AWARENESS IN CND

Task and system factor in relation to non-functional design requirements to computer network security (CNS) and computer network defence (CND) are discussed. This list is by no means exhaustive, however, the necessary steps toward understanding the essential attribute to designing and implementing SA in computer network security have been strategically presented (see *Figure 2*), as follows:

### DYNAMISM

The dynamics of SA was suggested by Endsley M. 1995, but generalised by Garba D. M., and Howard S. K., 1995. They compared SA requirements in aviation to that of anaesthesiology, and found that both fields are similar in characteristics, such as dynamism, complexity, high information load, variable workload and risk (Breton R., and Rousseau R., 2003). This made it possible for SA to be investigated with the same methods in both fields. Interestingly, computer network is analogous to both aviation and anaesthesiology in exhibiting similar characteristics. Computer network is a collection of interdependent systems whose operations are dynamic and often complex. They output huge information (logs), have variable and abrupt workload (traffic) and various associated risks.

I. *Dynamic:* the operation of network objects and computing devices is fast-changing, continuous and dynamic. For instance, network traffic being monitored is abrupt in nature and changes over time due to on-going activities in the network; traffic re-route is dynamic too.

II. *Volumetric information load:* logs and alerts produced by network objects, such as IDS, firewalls, routers, switches and servers are huge, diverse and significant. Often times, these logs are archived and may be required to be kept for several months as stipulated by the prevalent data retention, security compliance standards, archival and retrieval laws. In essence, computer networks are characteristically of high information load, significant logs and carry huge volumes of traffic.

III. *Abrupt in nature and variable workload:* network traffic is abrupt and varied in nature, often within expected baselines and acceptable service level agreements (SLAs).

IV. *Risk:* vulnerabilities exist in most computing systems, either in the form of flaws in software or the absence of protection controls, such that threats exploit these vulnerabilities to consequently attack computer systems and networks. Risk may result from faults, failures and errors in computing operations. E.g., errors due to human input, deliberate omission, faults that occur during operations or failures that happen when an adversary perpetuates computing systems.

Dynamic and complex environments were the interest of early work carried out in the field of situation awareness; primarily because, these fields were very susceptible to risks, human errors, faults and failures in systems. As such situation awareness is not applicable or of interest in static, or tightly controlled environments as shown by Anderson H. H. K., and Hauland G., 2000.

It has been suggested that some fields are not SA compliant, for example, results from the nuclear power plant process control was less fruitful. It is believed that operations of nuclear power plant processes were perfectly executed, hence offered no opportunity to make mistakes, and then few opportunities to observe fluctuations in SA (Breton R., and Rousseau R., 2003).

## COMPLEXITY

By their very nature, some environments are complex. This is particularly true with computer network defence. Computer networks are characteristically complex, some spanning across many distributed wide area networks (WANs) and geography, whilst using technologies to implement complex business logics and engaging in electronic transactions. At a high-level, computer networks will comprise a number of network objects, element managers, and localised and transient computing devices. For example, a computer network may comprise intrusion detection systems, firewalls, anti-malware (anti-virus, anti-SPAM and anti-phising systems), identity management systems, servers, workstations, PCs, switches, routers, PDAs etc. Networks are usually interconnected, with several interconnectivity points; for instance, interconnection with an ISP, partner organisation, vendors and users (telecommuters, and teleworkers). To effectively manage these assets and in addition to managing interdependent risks resulting from in network connectivity (physical, logical, spatial) in time and space is complex and challenging. Hence, it is challenging for administrators to maintain situational awareness over thousands of network objects and events (Gregoire M. and Beaudoin L., 2005).

## HETEROGENEITY

Heterogeneity is the ability of the security analyst to use different heterogeneous sources to observe, gather and detect dynamic changes in the network. E.g., the use of IDS, firewalls, anti-virus systems and security guards to collate security information observed in the network. The idea of using heterogeneous controls assists to create a true situational awareness, since no single control is able to identify all security threats, therefore, it is recommended to use heterogeneous controls in order to detect a wide-range of threats and attacks perceived in the

network, which is not possible from a single control perspective. Heterogeneity as a situation awareness attribute was suggested by Lefebvre J. H., et al., 2005; Liu X. 2007; and Gregoire M. and Beaudoin L., 2005 using heterogeneous controls in C2.

## SCALABILITY

Scalability is a system requirement, which is used to determine the performance of that system under varying loads, and to deduce how that system would react (handle, perform or degrade) under growing load in future. Scalability denotes the ability to accommodate a growing load in the future (Emmerich W., 2000). This means when designing CND applications, systems and software, including networking infrastructure should be tested to ensure they can cope with the ever-increasing CND demand. The emphases for systems designers is to ensure that CND systems and architectures are scalable, and support the organisation's mission, and do not contribute to degradation, error or loss of situational awareness. The primary basis for computer network defence is to provide secure, reliable and operational platform for an organisation (Onwubiko C., 2009), by focusing on managing the vulnerabilities and risks inherent in all computer networks (Lefebvre J. H., et al., 2005). Hence, if the sole purpose of the CND is defeated due to performance bottleneck of its own system's or architecture, then it is highly unlikely that operators' situational awareness is enough to support mission critical objectives.

By default, systems and network devices produce high volumes of logs, running significant processes, and analyse huge amount of traffic, handle a significant number of concurrent users, and processing distributed transactions and services, making a computer network defence environment demanding and challenging. Therefore, it is characteristically important that CND systems and infrastructure designs are scalable and distributed to support the dynamic and demanding operational activities of the environment.

## OPENNESS

Openness is a non-functional property of a network, system or software when it complies with well-defined and documented standards (a.k.a. open standards). Open systems are systems that can be easily extended and modified either as a whole or component-wise. A key benefit of an open system is that it is built from components that can be readily removed and replaced with multiple-sourced alternatives and so many suppliers can compete for that business (Henderson, P., 2007).

Openness is demanded because the overall architecture needs to be stable even in the presence of changing functional requirements (Emmerich W., 2000). The integration of new components to this system means that they have to be able to communicate with some of the components that already exist in the system. This is the whole essences of having components with well-defined interfaces.

The relationship of openness to CND systems is that CND systems need to be designed with open standards, such as GIS systems, protective monitoring systems, and modern CPS systems such that when a component becomes unavailable, its change or replacement does

not put the entire CND environment into unprecedented difficulty, and consequently hinder the operators the capability to respond to ongoing situations in the network.

### RESOURCE SHARING

Resource sharing is a typical non-functional requirement of distributed systems such as a computer network defence environment, where multiple users concurrently share the same CND data, hardware or software components. While resource sharing in CND is an essential design requirement, however, access control of shared resource is a concern. Access to shared resource must be controlled, restricted and assessed. The sensitive and criticality of CND operations and dynamic nature of this environment make access control not only for share resources, but also of the entire platform a necessary and essential control requirement.

### FAULT TOLERANCE

Network infrastructure, systems and software occasional fail. Some fail because of software error, programming issues, failures in the underlying infrastructure (for example, power failure or air conditioning), abuse by their users, attacks from an adversary, or just because of ageing hardware. For example, the lifetime of a hard disk lies between two and five years, much less the average lifetime of a distributed system (Emmerich W., 2000).

An essential non-functional requirement that is often demanded from a system is fault-tolerance. That is the ability of a system to continue to operate, even in the presence of faults. This in our opinion is a must-have requirement for computer network defence systems given the important roles they perform, and the business-critical tasks required by missions, institutions and organisations.

Modern computer network defence systems that are designed for situational awareness must not just be fault tolerant; they should also be fail-secure. Fail-secure is a non-functional requirement of a system to close all its channels when it fails. A fail-secure system is one that, in the event of failure, responds in a way that will cause no harm, or at least a minimum of harm, to other devices or dangers to personnel. For example, a fail-secure firewall system is a firewall system that when it fails, does not allow all traffic destined to the network through; rather it denies all traffic. There are variants of fail-secure systems such as fail-close, fail-open, and fail-safe. CND systems should be designed to be both fault-tolerant and fail-secure.

## CONCLUSIONS

Situational awareness as a human factor attribute can be enhanced through a number of ways, such as individual factors (operator abilities, training and experience),workload, stress, goals; and task and system factors, such as the use of technology (interface design, integration, analysis and processing to enrich SA, as shown in Figure 1.

In this chapter, we have investigated task and system design requirements that enables enhance situational awareness in CND. These requirements are decomposed into functional and non-functional design requirements, each area covering both task and system-specific attributes. The contribution of this chapter will underpin the design construct of new and

modern computer network defence systems that are able to extend the boundary that already exist, and become foundation for a roadmap that could eventually lead to advances in the CND situational awareness.

There are a good number of contributions in the literature focusing on technical and analytical contributions to computer network defence and situational awareness. Unfortunately, not very many contributions are published that discusses qualitative requirements, especially, system and task related factors pertinent to CND specifically. Existing contributions are in mainstream SA areas such as air traffic control, aviation and warfare. Our contribution is a comprehensive assessment of pertinent factors to be considered when designing modern computer and network systems for situational awareness in a CND environment. We covered a good breadth of both non-functional, and functional system requirements, and also, task-oriented requirements which are partly associated to both human and system.

Our future goal is to investigate human specific design requirements for enhance situational awareness in CND, which should complements this contribution.

## REFERENCE


Anderson H. H. K., and Hauland G., (2000), "Measuring Team Situation Awareness of Reactor Operators during Normal Operation: A Technical Pilot Study", Proc. of the first Human Performance, Situation Awareness, and Automation Conference, Savannah, 2000.

Bass T., (2000), "Intrusion Detection Systems and Multisensor Data Fusion", *Communications of the ACM, **Vol. 43, No.** 4, 2000*

Borja A. T. (2003), "Integrating Usability Engineering in the Iterative Design Process of the Land Attack Combat System (LACS) Human Computer Interface", Space & Naval Warfare Systems Center, San Diego, CA 92152-5001, USA, 2003.

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

Breton R., and Rousseau R., (2003), "Situation Awareness: A Review of the Concept and its Measurement", DREV, TR-2001-220, Defence Research Establishment, 2003.

Carnegie Mellon, (2005), SILK: System for Internet Level Knowledge (SILK), Carnegie Mellon SEI, CERT NetSA Security Suite, 2005. [Accessible from] http://tools.netsa.cert.org/silk/. (Accessed 29th March 2011).

Cisco Systems Inc, (2011), Cisco ASA 5500 Series Adaptive Security Appliances, [Accessible from] http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_brochure0900aecd80285492.pdf

D'Amico A. and Kocka M., (2005), "Information Assurance Visualisation for Specific Stages of Situational Awareness and Intended Uses: Lessons Learned", *Workshop on Visualisation for Computer Security, USA, 2005.*

Emmerich W., (2000), Engineering Distributed Objects, John Wiley & Sons, Ltd, England, UK, ISBN: 0-471-98657-7

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

Endsley M. R., (1996), "Automation and Situation Awareness", Automation and Human Performance: Theory and Applications, pp. 163-181, NJ, 1996.

Endsley M. R. and Garland D. J., (Eds) (2000), Situation Awareness Analysis and Measurement; Mahwah, NJ; Lawrence Erlbaum Associates, ISBN: 0-8058-2133-3, 2000.

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.

ESRI (2008), "Public Safety and Homeland Security Situational Awareness", An ESRI White Paper, February 2008 [Accessible from] www.esri.com

Garba D. M., and Howard S. K., (1995), "Situation Awareness in Anaesthesiology", *Human Factors, **Vol. 37, Issue 1, pp. 20-31**, 1995.*

Gregoire M. and Beaudoin L., (2005), "Visualisation for Network Situational Awareness in Computer Network Defence", Proceedings of the *Visualisation and the Common Operational Picture, pp. 20-1-20-6, RTO-MP-IST-043*, 2005.

Hall D. L., and McMullen S. A. H., (2004), "Mathematical Techniques in Multisensor Data Fusion", 2nd Edition, ISBN: 1-58053-335-3, 2004

Haines J., Ryder D., Tinnel L., and Taylor S., (2003), "Validation of Sensor Alert Correlators", *IEEE Security & Privacy, **Vol. 1, No. 1,** pp.46-56, Jan-Feb. 2003.*

Henderson, P., (2007), "On Open Systems and Openness", University of Southampton, October 30th 2007. [Accessible from] http://pmh-systems.co.uk/OpenSystems/ OpenSystems.pdf [Accessed 26th April 2011]

Juniper Networks, (2011), IGS Series Integrated Security Gateway, [Accessible from ] http://www.juniper.net/us/en/local/pdf/datasheets/1100036-en.pdf#xml=http://kb.juniper.net/index?page=answeropen&type=open&searchid=1255112038522&answerid=16777216&iqaction=6&url=http%3A%2F%2Fwww.juniper.net%2Fus%2Fen%2Flocal%2Fpdf%2Fdatasheets%2F1100036-en.pdf&highlightinfo=18875208,1477,1492 [Accessed 25th April 2011]

Lakkaraju K., Yurick W., and Lee A. J., (2004), "NVisionIP: NetFlow Visualizations of System State for Security Situational Awareness", NVisionIP, *VizSEC/DMSEC'04,* October 29, 2004, Washington, DC, USA, 2004

Lambert D. A., Bosse E., Breton R., Rousseau R., Howes J. R., Hinman M. L., Karakowski M., Owen M., and White F., (2004), "Information Fusion Definitions, Concept and

Models for Coalition Situation Awareness", *TTCP C31 Group, TR-C31-AG2-1-2004,* 2004.

Lee E. A., (2006), "Cyber-Physical Systems – Are Computing Foundations Adequate?", Department of EECS, UC Berkeley, NSF Workshop on Cyber-Physical Systems: Research Motivation, Techniques and Roadmap, October 16-17, 2006

Lefebvre J. H., Gregoire M., Beaudoin L., and Froh M., (2005), "Computer Network Defence Situational Awareness Information Requirements", Defence R&D Canada, Ottawa, TM 2005-254, 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.*

Mulgund S., Rinkus G., Illgen C., and Zacharias G., (1997), "Situation Awareness Modelling and Pilot State Estimation for Tactical Cockpit Interfaces*", Presented at HCI International, San Francisco, CA, August 1997*

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 Publisher, ISBN: 978-3-639-08934-9, 2008.

Onwubiko C., (2009), "Functional Requirements of Situational Awareness in Computer Network Security"; Proceeding of the IEEE International Conference on Intelligence and Security Informatics, IEEE ISI 2009, 8-11, June 2009, Dallas, Texas, USA.

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*.

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.

Sandom C., (1999), "Situational Awareness through the Interface: Evaluating Safety in Safety-Critical Control Systems", *IEE Proceedings of People in Control – An International Conference on Human Interfaces in Control Rooms, Cockpits and Command Centres, University of Bath,* UK, 21-23 June 1999.

US FAA, (1991), "Aeronautical Decision Making", U.S. Federal Aviation Administration (FAA) Advisory Circular (AC) 60-22, 1991

Wickens C. D., (1992), "Engineering Psychology and Human Performance", 2nd Edition, New York, Harper Collins, 1992.

Yin X., Yurick W., and Slagell A., (2008), "VisFlowConnect-IP: An Animated Link Analysis Tool for Visualising Netflows", SIFT Research Group, National Centre for Supercomputing Applications, University of Illinois at Urbana-Champaign, 2008.

Yurick W., (2005), "Visualising Netflow for Security at Line Speed: the SIFT tool suit", *Proc. of the 19th Usenix Large Installation System Administration Conference (LISA), pp. 169-176, 2005.*

## ADDITIONAL READING SECTION

Onwubiko C., (2008). *Security Framework for Attack Detection in Computer Networks*. Germany: VDM Publishing.

Onwubiko, C., (2011). Modelling Situation Awareness Information and System Requirements for the Mission using Goal-Oriented Task Analysis Approach. Chapter Contribution in Situational Awareness in Computer Network Defence: Principles, Methods and Applications, IGI Press, 2011 (*in press*).

Juarez-Espinosa, O. and Gonzalez, C. (2004). Situation Awareness of Commanders: A Cognitive Model. Department of Social and Decision Sciences, Paper 85, 2004.

Bares, D. (2010). A Tactical Framework for Cyberspace Situational Awareness (Paper #196). Topic 8: C2 Assessment Metrics and Tools, Air Force Institute of Technology, AFIT/ENG, 2010.

Gruber D. J. (2000). Computer Networks and Information Warfare – Implication for Military Operations. Occasional Paper No. 17 Center for Strategy and Technology Air War College, Air University Maxwell Air Force Base, 2000.

## KEY TERMS & DEFINITIONS

Computer Network Defence: CND is the process of protecting computer systems and networks. This includes actions taken via computer networks to protect, monitor, analyse, detect and respond to cyber-attacks, intrusions, disruptions or other perceived unauthorised actions that could compromise or impact defence information systems and networks. CND is achieved through a collective effort by personnel who monitor, manage and maintain defence systems, networks and infrastructures, such as network operators, security analysts, systems administrators and IT support.

Situation Awareness: SA is the process of perceiving the elements in the environment, understanding the elements in the environment, and the projection of their status into the near future (Endsley M. R., 1996).

Functional Requirements: These are requirements and functions that the system performs for its users such as processing, display, tasks and analysis.

Non-Functional Requirements: Non-functional requirements are concerned with the quality of the system. They are, rather, global system qualities; hence non-functional requirements typically have serious impact on the overall architecture of the chosen system.

## KEYWORDS

Situation Awareness, Computer Network Defence, Design Requirements, Functional Requirements, Non-functional Requirements, Network Security, Multi-sensory Data Fusion, Human Factor