Active Offensive Cyber Situational Awareness: Theory and Practice

A thesis submitted for the degree of Doctor of Philosophy

By
Ahmed Al-Shamisi

College of Engineering Design and Physical Sciences
Department of Computer Science
Brunel University

August 2014

ACKNOWLEDGMENTS

The completion of my PhD thesis has been a long journey. It's true that "Life is what happens" when you are completing your PhD thesis. Life doesn't stand still, nor wait until you are finished and have time to manage it. Much has happened and changed in the time I've been involved with this project, or as some of my dear friends have so affectionately referred to it "The Paper." This PhD thesis could not have been completed without the great support that I have received from so many people over the years. I wish to offer my most heartfelt thanks to the following people

To my supervisor, mentor and friend Professor Panos Louvieris, Thank you for the advice, endless support, and willingness that allowed me to pursue research on topics for which I am truly passionate. I see the same drive and passion in your own research efforts, and I thank you for letting me do the same. Thank you for all of the meetings and chats over the years. You recognized that I at times needed to work alone but also made sure to check in on me so that I stayed on the right path.

To my Mother and Father, without whose love, encouragement and support assistance, I would not have finished this thesis. You have encouraged my academic interests from day one. Thank you.
In addition, these acknowledgements would not be complete if I did not mention my wife and daughter. She has been a twinkle in my eye since she was born.

A very special thanks goes out to my friends and colleagues at Brunel university, which helped me throughout the years in exchanging of knowledge and skills during my graduate program, which helped enrich my experience.

My gratitude is also extended to my sponsor, Abu Dhabi Police General Head Quarters for the endless support and for believing in me and sponsoring this research from the beginning.

DECLARATION

I, Ahmed Al-Shamisi, declare that this thesis is the result of my own independent work/investigation, except where otherwise stated. Other sources are acknowledged by explicit references. The views expressed are my own. This work has not been submitted in substance for any other degree or award at this or any other university or place of learning, nor is being submitted concurrently in candidature for any degree or other award.

ABSTRACT

There is an increasing gap between the progress of technological systems and the successful exploitation of these systems through cyber-attack. Whilst the mechanism and scope of cyberspace is progressing with each passing day, risk factors and the ability to process the required amount of data from cyberspace efficiently are proving to be major obstacles to achieving desired outcomes from cyber operations. This, coupled with the dramatic increase in the numbers of cyber attackers, who are constantly producing new ways of attacking and paralysing cyber systems for political or financial gain, is a critical issue for countries that have linked their major infrastructures with Internet applications. The defensive methods currently applied to counter these evolving attacks are no longer sufficient, due to their preventive and reactive nature. This research has developed a new Active Situational Awareness theoretical model for Active Defence that aims to enhance the agility and quality of cyber situational awareness in organisations in order to counter cyber attacks.

Situational Awareness (SA) is a crucial component in every organisation. It helps in the assessment of an immediate situation in relation to the environment. Current SA models adopt a reactive attitude, which responds to events and works in passive manner to any progressing enemy cyber attack. This creates a defensive mind-set and consequently influences the operator to process and utilise knowledge only within the concept of attack prevention. Thus, one can assume that operators will only gather certain knowledge after the occurrence of an attack, instead of actively searching for new intelligence to create new knowledge about the cyber attack before it takes place.

This research study introduces a new approach that incorporates an Active Defence posture; namely, a 'winning attitude' that conforms to the military stratagems of Sun Tzu, where operators always engage attackers directly in order to create new knowledge in an agile manner by deploying active intelligence-gathering techniques to inform active defence postures in cyberspace. This also allows the system being protected to remain one step ahead of the attackers to ultimately defeat them and thwart any costly attacks.

To back these statements, this study issued a survey to 200 cyber defence and security experts in order to collect data on their opinions concerning the current state of Active SA. Structural Equation Modelling (SEM) was then employed to analyse the data gathered from the survey. The results of the analysis revealed significant importance of Active Offensive Intelligence gathering in enhancing Cyber SA. The SEM showed there is a significant impact on SA Agility and Quality from Active Intelligence gathering activities.

Further to this, the SEM results informed the design of the serious gaming environments utilised in this research to verify the SEM causality model. Also, the SEM informed the design of a SA assessment metric, where a behavioural anchor rating scale was used along with ground truth to measure

participant SA performance. The results of this experiment revealed that there was 2 times better enhancement in cyber Situational awareness among those who did utilise active measures compared with participants who did not which mean almost double and this shows the importance of offensive intelligence gathering in enhancing cyber SA and speed up defender decision making and OODA loop.

This research provided for the first time a novel theory for active cyber SA that is aligned with military doctrine. Also, a novel assessment framework and approaches for evaluating and quantifying cyber SA performance was developed in this research study. Finally, a serious gaming environment was developed for this research and used to evaluate the active SA theory which has an impact on training, techniques and practice

Deception utilisation by Active groups revealed the importance of having deception capabilities as part of active tools that help operators to understand attackers' intent and motive, and give operators more time to control the impact of cyber attacks. However, incorrect utilisation of deception capabilities during the experiment led operators to lose control over cyber attacks.

Active defence is required for future cyber security. However, this trend towards the militarisation of cyberspace demands new or updated laws and regulations at an international level. Active intelligence methods define the principal capability at the core of the new active situational awareness model in order to deliver enhanced agility and quality in cyber SA.

TABLE OF CONTENTS:

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

1.0 INTRODUCTION

The world of cyber operations has reached a crisis point, where on the one side operational technology is progressing at a breakneck speed, while on the other risk factors are increasing at an equivalent rate due to increased hacking activities. For example, since Web 2.0 there has been a proliferation of cyber attacks (Orielly, 2005). Several countries have reported major damage caused by cyber attacks, which include complete destruction of critical national infrastructures, severe disruption to financial activities and other essential services (power, telecommunications, air traffic management, etc), as well as theft of national security data. The magnitude of the crisis can be tracked back to instances of the suspected involvement of governmental agencies in exploiting the weak security infrastructure of other countries to cause damage, or for unlawful gains.

For example, the Iranian government has already held the US and Israel responsible for masterminding the Stuxnet (computer worm) attack on its uranium enrichment centrifuges (Greenwald & MacAskill, 2013), while Syria has openly deployed a hacker group named the 'Syrian Electronic Army' that is engaged in bringing down, defacing or otherwise maligning any sites that carry anti-Syrian government content (Norman, 2011).

Similarly, China has also been found to be steadily increasing its espionage network in recent times, according to the report furnished by SecureWorks, a leading security services provider, which recorded 7.7 million attempted attacks from China in 2008. At the same time, China has also released a hacking toolkit onto the market named 'Leopard in a Hole', which is available at a price ranging from $20 to $500, and which can help in penetration tests that are used to identify and exploit SQL injection flaws (Dwyer, 2009). This state of affairs clearly has precipitated a new era in global cyber warfare, which might be more devastating than what the world witnessed in the earlier world wars.

The basic reason why this state of affairs exists stems from the fact that hackers enjoy huge advantages when dealing with traditional cyber security practices, since in these cases they remain in a position to decide on the place, time and method of attack. The defender who is a victim of these attacks cannot easily gather any clues about impending attacks, as a result of adopting a passive defence posture. From a cyber security perspective, this passive, handicapped state of the defenders hinders their Cyber Situation Awareness (SA). At this point, the issue of attitudes becomes very pertinent, since it is the defensive attitude of the defenders that prompts them to react after the occurrence of an attack, thereby losing the battle at the very first round. The current cyber security controls described above are inadequate to counter these evolving cyber attacks, due to their preventive and reactive nature. The passive approach currently adopted in cyber security only allows defenders to react after a cyber incident, which is to all intents and practical purposes too late because the effect has already taken place.

With this in mind, if one considers cyber warfare to be an important and integral component of contemporary warfare then one cannot neglect the importance of adopting a winning, active attitude. This is necessary to remaining always one step ahead of the attackers in terms of military strategy and execution. From the perspective of cyber security, this winning, active attitude can be termed 'active defence', whereby defenders should always engage the attackers by exploiting active intelligence-gathering techniques by constantly creating and utilising new knowledge to ensure impenetrable protection of cyber infrastructures. However, this proposition requires validation through reliable measures and critical assessment. With this in mind, this study critically investigates the efficacy, efficiency and effectiveness of its own active defence model, one that conforms to the military stratagems of Sun Tzu, the legendary military strategist of yesteryear, to ascertain whether this model is more capable of enhancing SA agility and quality than the existing traditional SA models.

This research explores state-of-the-art SA by investigating the existing SA models and identifying their limitations when applied in the cyber domain. The main goal of this research is to introduce a new theoretical framework for active cyber SA and demonstrate its value for enhancing overall cyber SA in practice through serious gaming experiments. Drawing on the expertise of cybersecurity subject matter experts from across the world, Structural Equation Modelling (SEM) is used in this research to verify the causality of the new theoretical model and to test whether and to what extent active offensive intelligence-gathering enhances cyber situational awareness agility and quality while handling a cyber incident. A serious gaming environment, a cyber range testbed, was developed to: (i) facilitate the assessment of participants' SA when the new active SA theory is employed in practice; and (ii) specifically test whether participant cyber SA is enhanced when an active offensive capability is introduced. For that purpose, a behavioural anchor rating scale was used, and a cyber SA assessment framework was developed based on the findings of the SEM.

1.1 Research Background/Problem Statement

Steady growth in cyber crime has been observed since the mid-1980s, and the present situation has reached a state where cyber attackers hold enough power to destroy the critical infrastructures of any nation (e.g. power, telecommunications etc). The growth rate of cyber crime further consolidates the above view. In 2008, the FBI found a 33% rise in individual crime complaints in their investigation (Rowe & Rothstein, 2004), while Symantec, the maker of the famous Norton anti-virus system, found and blocked 5.5 billion malicious attacks in 2011, which is 81% higher than the volume of such attacks they found and blocked in 2010. And the finding of most concern is that the majority of such attacks targeted social networks and mobile phones (Albanesius, 2012).

However, it is not that the experts were not tracking the cause of the above phenomenon. In the 1990s, the experts (Endsley & Kiris, 1995; Sarter & Woods, 1995) identified it as an outcome of the increasing gap between the progress of systems and successful exploitation of the same, which can be termed as a mismatch between the required and existing levels of SA. They also pointed out that it has

become virtually impossible to cope with the increasing dynamism of cyber technology and lethality of cyber attacks without quality SA. The inability to interpret the environment and be able to answer the fundamental question about the cyber situation among cyber operators, allows the disruptive abilities of cyber attackers to cause damage, and sets the current balance of cyber power in favour of the attackers Geers (2011).

The gravity of the consequences suffered from the absence of an established way to redefine the current Computer Network Operation (CNO) in achieving SA could result in horrific breakdown of cyber infrastructures that help run all critical infrastructures across the globe. This is illustrated by the following instances of cyber attacks and their associated consequences:

- In 2001, a 15-year-old hacker nicknamed MafiaBoy worked his way into the portals of top online companies and caused over US $1 billion financial losses (Verton, 2002);
- In 2007, Israeli cyber attackers intruded into the Syrian Air Defence ICT infrastructure and deactivated it, which enabled them to demolish the Syrian nuclear reactor (Fulghum, Wall & Butler, 2007);
- This attack prompted Syria to form the 'Syrian Electronic Army', which is a hacker group that is engaged in bringing down, defacing or otherwise maligning sites that carry anti-Syrian government content;
- Israel and the US allegedly masterminded the Stuxnet computer worm attack on Iranian uranium enrichment centrifuges in 2010 (Greenwald & MacAskill, 2013);
- This attack prompted Iran to respond with its 'Iranian Cyber Army' (Rudner, 2013);
- The Mandiant Report published by a US agency showed that cyber espionage by PLA (China) had been hacking the *New York Times*' computer systems since 2012 to mid-2013 (Feakin, 2013);
- The US drew up a list of potential overseas targets for US cyber attacks within a project named 'Offensive Cyber Effects Operations' (OCEO), which clearly suggests that the US government is stepping up its cyber offensive capabilities (Greenwald & MacAskill, 2013).

The above instances highlight the fact that critical political, social and financial operations with a cyber dimension can be brought down from a totally unknown quarter and for unknown reasons. Further, it substantiates the fact that cyber security should evolve from "a technical discipline to a strategic concept" (Geers, 2011: 9), in the way that any strategic challenge requires strategic solutions. Moreover, when looking into these problems, there is no theoretical cyber SA framework or practical model that addresses the problems discussed herein. At this point, one realises the shortcomings of the traditional SA models, which are driven by a passive attitude of preventing cyber attacks. Hence, there is a clear need to adopt an active approach to cyber SA that would apply new knowledge gained from cyber intelligence gathering activities along with other prior knowledge to engage the attacker in a manner that takes advantage of this new knowledge. It is only recently that active defence has come to prominence and is being discussed more openly in public, and so adopting this approach to cyber SA

could change the balance of power between players. However, due to the legal and political restrictions on applying active SA, this research has developed a serious gaming environment that provides a legitimate environment in which to experiment and test the validity of active SA theory and practice so that no law was broken while pursuing this research. Active defence is a force multiplier in the defence of a realm, and the ultimate question is whether nations can afford not to take up active SA, given the national strategic importance of protecting high value assets like the Critical Network Infrastructure (CNI) of a nation's economy and its day to day operation, or stay passive and allow cyber attackers who have adopted the active method to cause disruption to the nation.

1.2 Research Aim and Objectives

The aim of this research is to investigate whether an active offensive approach is more capable of enhancing cyber SA agility and quality than the existing SA models. This aim stems from an ultimate aim of contributing to the understanding of the concept of cyber situational awareness as well as deriving new cyber capability. Accordingly, the study contains five objectives:

1. Determine and critically analyse the current SA models and identify the key dimensions and variables for active cyber SA;
2. Develop a theoretical framework for active SA
3. Evaluate active SA deployment in a serious gaming environment;
4. Develop a method framework for assessing cyber SA; and
5. Empirically assess the significance of effect and implications of active defence in enhancing cyber SA agility and quality.

1.3 Research Significance

The significance of this research rests on certain presumptions: that it would cover the gap in the existing literature, would prevent losses of various dimensions and magnitudes, would contribute to the process of creating a power balance among countries, and would ensure safety in all commercial and general cyber transactions for individuals and organisations.

This study has found no literature that emphasises adopting a winning/proactive attitude while utilising SA in protecting cyber systems, or any literature that recommends utilising an active SA model for the same purpose. From these perspectives, this study stands unique. Similarly, it can be said that successful deployment of the new active cyber SA model developed in this research will enable the operators of cyber systems to increase the likelihood of successfully deterring cyber attacks, which in turn will save them from any associated losses that might take place otherwise. Alongside this, it can be easily assumed that the possession of the proposed active SA model will create a power balance among countries, since possession of the same will bolster the SA of all countries, where no one country will be able to attack another country by exploiting its weak SA. Similarly, implementation of this model in practice will enable all organisations and individuals to seamlessly operate in the cyber world, as it will maximise protection for them.

1.4 LAY OUT OF THESIS

Chapter 2 of this study is designed to explore the literature in the area of cyber security, defence and situational awareness in order to develop and design a theoretical, hypothesised framework for active offensive cyber SA and make the case for active defence. This is achieved by providing a brief background about cyber security issues that shows how the current cyber security counter initiative is not sufficient for facing the current evolved cyber environment due to its passivity. Also, it shows why an active, offensive approach that adopts military philosophy is better for enhancing cyber security. The legal aspect of self-defence is also discussed in this chapter and different examples are given to make the case for active SA.

Chapter 3 begins a review of research methodologies. In turn, the chapter seeks to filter through the methods and select a handful of methods and, where necessary, establish a combination of them and/or set out a procedure determining which method to use and when. Within this chapter, data analysis techniques are discussed, as this research utilises SEM to verify the hypothesised theoretical framework, which are then used to develop the serious gaming environment (discussed in this chapter in detail), a SA awareness behavioural anchor rating scheme, and a SA measurement framework and marking scheme based on simulated ground truth. This chapter also provides the type of instrument used to collect data, and the method of analysis.

Chapter 4 analyses the structural equation modelling of the hypothesised theoretical framework discussed in chapter two using the data collected from the electronic survey (Appendix 1). The structural model was produced after this research had conducted several types of test prior to the exploratory factor analysis. Then, confirmatory factor analysis was conducted to test the consistency of the construct and to determine whether the data fit the hypothesised measurement model.

Chapter 5 explores the analysis of the experiments' results conducted using the serious gaming environment to test whether active offensive cyber intelligence could enhance cyber SA. Also, additional tests were conducted to test the impact of education, the utilisation of deception and the utilisation of offensive hacking in enhancing cyber SA. Independent Sample T-Test and One-Way ANOVA were used in this analysis.

Chapter 6 critically discusses the findings previously covered in chapters two, four and five, and provides a justification for how active offensive cyber intelligence could enhance cyber SA agility and quality. The main theoretical contribution of this research is a novel and robust approach and framework for cyber SA where for the first time an active offensive intelligence activity that aligned correctly with military doctrine is integrated into the SA model which provides quality information that enhance the agility of awareness. Methodologically, this research provided a serious gaming environment as a robust testing environment that enabled this research to run cyber war game to test the impact of active SA model in enhancing cyber security. Also, an assessment framework was

developed using the power of statistic for the first time to evaluate the efficiency, efficacy and effectiveness of individual's cyber SA. Finally, this chapter discusses the limitations and issues that might follow the adoption of an active offensive approach. Finally, recommendations and a conclusion are provided at the end of this research.

CHAPTER 2: LITERATURE REVIEW

2.0 OVERVIEW

Since the mid-1980s, experts on cyber systems have been observing an increasing gap between the progress of systems and successful exploitation of the technology. While the mechanisms and scope of the cyber world have been leaping forward with each passing day, risk factors and the need to process the required amount of data from the ocean of information in less time and with less effort are proving major roadblocks to achieving desired outcomes from cyber operations. Altogether, the experts (Tadda et al., 2006; Sudit et al., 2005; Dutt et al., 2013) point to the following two factors that demand quality cyber situational awareness, and the ability to apply the same, from its operators:

- Coping with increasing dynamism of cyber technology
- Coping with increasing lethality of cyber attack

The first factor, i.e. coping with increasing dynamism of cyber technology, has reached a point where it has become almost unmanageable for cyber operators without quality situation awareness. The second factor is increasingly becoming a nightmare for those countries that have already associated their major infrastructures with Internet applications, as the population of cyber attackers has dramatically increased. They are constantly producing novel ways of attacking and paralysing cyber systems for criminal or terrorism gains, e.g. political or financial gains where active defence is more likely to be justified when cyber attacks are against CNI.

It would be pertinent to recall that the aim of this study is to ascertain whether an all-pervasive, Active SA Model (henceforth ASAM) proposed in this research can save time, increase productivity and empower the end user to remain always one step ahead of their enemies in any cyber situation. Therefore, this aim also governs the structure and content of the literature review. This chapter reviews the background and the present state of SA research in order to determine the salient variables of existing SA models and their shortcomings, which will inform the methodology for validating the proposed ASAM.

This chapter explores the current literature in the areas of cyber security and defence, and situational awareness, covered in five main sections. In the first section, a brief background about the cyber threats and cyber security issues is set out that shows how current cyber security counter initiatives are not sufficient for the current evolved cyber environment. Also, this section provides an insight into military doctrine, showing how military science could be utilised to enhance cyber security. The second section explores current SA models and critically reviews their variables to determine the shortcomings of current SA model when deployed it in the cyber domain. Also, this section exposes the problem with the current passive approach, and why cyber SA needs to adopt an offensive, active approach to deterring cyber incidents. At the end of this section, a legal aspect about cyber self defence is covered

that explores different countries' laws when it comes to cyber defence. The third and fourth sections, critically synthesises the main points from the literature reviewed the previous section, and makes the case for active cyber SA. A hypothetical, theoretical framework is provided for ASAM, and a process model is developed. Finally, a summary of this chapter is provided in the fifth section. This chapter thus aims to critically review the current literature in order to develop and design a hypothesised theoretical framework for active cyber SA and make the case for active defence.

2.1 BRIEF BACKGROUND

2.1.1 Evolved Cyber Environment

The disruptive abilities of the cyber attackers have influenced cyber security, causing it to evolve from "a technical discipline to a strategic concept" (Geers, 2011), since strategic challenges demand strategic solutions. The significance of the same lies in the fact that all political, social and financial functions today have a cyber dimension, where they always run the risk of getting attacked from totally unknown quarters, and for unknown reasons. Consequently, the entire system could collapse, or, worse, sensitive data could be stolen without the knowledge of the operator, and these data could then be exploited against the country to which the operator belongs.

Geers (2011) categorically states that the current balance of cyber power favours the attacker. It is for this reason that world leaders (the G8) have increasingly expressed their worries regarding system breakdown or cyber espionage (Cody, 2007). An investigation into cyber crime conducted by the FBI in 2008 found a 33% rise in individual crime complaints, which was tantamount to $264.6 million (Rowe & Rothstein, 2004). Altogether, cyber attacks, under the name of 'information warfare', have become commonplace events since early 1990s and were later dubbed as strategic warfare (Molander et al., 1998: 3), before earning two more nicknames: cyberwar and netwar (Strategic Information, 2012). Cyberwar emanates from financial, political and fanatical aggression, all of which can leave a deadly imprint, as in the macabre instance of 9/11.

2.1.2 A Few Instances of Attacks

The visionary work of Rona (1976) regarding an information war suggested as early as 1976 that computer networks can be both an asset and a liability for an organisation, since their high utility value means they are liable to come under attack, and the information flow within any command-and-control system is bound to be vulnerable to jamming, overloading or spoofing by an attacker (Van Creveld, 1987).

The instances of abusing databases and networks to achieve military objectives started gaining momentum in the 1980s, when the Soviet Union launched its Military Technological Revolution (MTR). The gravity of cyber attacks lies in the fact that they can damage several systems in several ways, ranging from Denial of Service (DoS) to the destruction of critical infrastructure (Eichin & Rochlis, 1989; Mishra, 2003). For example, US President Obama announced in May 2009 that cyber attackers who had already disrupted power supplies in several countries were now probing those

countries' electrical grids (The White House, 2009). Obama's views were corroborated by journalists, who cited instances of cyber attacks in Brazil which affected millions of civilians in 2005 and 2007, where nobody could trace the origins of such attacks (Aitoro, 2009).

There are other instances, too. In 1999, unknown hackers tried to disrupt NATO military operations in the Kosovo war (Fulghum, 2006; Fulghumet al., 2007), while in 2007 an Israeli cyber attack paralysed the Syrian air defence network system right before its air force attacked a Syrian nuclear reactor (Fulghumet al., 2007; Lewis, 2002). In 2009, the Canadian research group named Information Warfare Monitor discovered GhostNet, a cyber espionage network comprising more than 1,000 computers across 103 countries that aimed to collect diplomatic, political, economic and military information (Information Warfare Monitor, 2009). In 2001, a 15-year-old student from Montreal, under the nickname MafiaBoy, caused over $1 billion financial damage to the top online companies by conducting a DoS attack (Verton, 2002). In another instance of DoS, the Burmese government blocked its entire network while cracking down on its political protestors (Tran, 2007).

The attack process in general involves steps such as reconnaissance, scanning, obtaining access, retaining access, covering tracks and hiding (Kjaerland 2005). According to Geers (2011), intention-wise cyber attacks can be categorised into three types:

I. Targeting confidential data
II. Targeting the integrity of information
III. Targeting the availability of information resources (DoS)

While the first type of attack aims to encompass any unauthorised acquisition of information by observing communication patterns, the second type of attack aims to sabotage data for criminal, political or military reasons. There are even instances of cyber criminals encrypting the data on a victim's hard drive and then demanding a huge ransom in exchange for the decryption key such as ransomware. The third type of attack aims to prevent authorised users from accessing their systems or the data required for performing certain tasks. This type is popularly known as a DoS attack. The main challenge facing cyber defence is that Internet technology evolves day by day, which makes it very difficult for operators to keep pace of the same (Geers, 2007a, 2011).

2.1.3 Basic Methods of Hacking

There are a number of methods that hackers use to invade computers that are online (Mitnick & Simon, 2002: 33). Often, it is hard to tell whether one's computer has been invaded until it is too late to remedy. In fact, the threat of zero day attacks raised this problem, where the zero day attack effect is unknown to the defenders. One truth that is not debatable is how resourceful, cunning and smart the computer invaders can be. Indeed, these con artists can even sometimes use one's weaknesses to invade the computers. Hackers are capable of getting into computers and tricking the owners into revealing sensitive information. In addition, they are also capable of getting onto the Internet and even

stopping the computer owners from accessing the Internet themselves (Erickson, 2008: 109). Hackers often target large companies; however, if individuals are in the wrong place at the wrong time they may also find themselves the targets. This is because the cyber attacker has the ability to take away the security, safety and peace of mind of the computer user (Bradley, 2006: 37). This raises a problem for home users who connect their home appliances (Internet of Things) to the network (house automation), where security controls are usually very basic due to performance restrictions. Moreover, the attackers have the ability to attack the computers regardless of the number of software that the users have installed to prevent them.

Social engineering is the driver of all cyber invasion activities (Wang, 2006: 178). In fact, scholars have noted that hacking and social engineering are like "two peas in the same pod" (Loch, Carr & Warkentin, 1992: 2). This is because hacking is the physical aspect, or rather the outcome, of the social engineering or 'mindset' of the invasion activities. At the outset, social engineering is a way in which the hackers can get information from their victims. The hackers can do this by knowing their victims or by winning their trust, and by making them comfortable enough so that they will give them all the information they need for the attack. Thus, based on the victims' responses, cyber hackers can choose to get quick information or use the longer route (e.g. hackers can collect intelligence about the target using passive methods where no interaction with target takes place, or use offensive scanning and social engineering to get into the target system without wasting their time looking for weaknesses to exploit). In addition, the hackers' choice of the route to take depends on the length of time the hacker has to devote to all of the work.

According to Adams (1990: 323), a good social engineer must not go into a person's computer to steal information; instead, the best approach would be to make the individual comfortable and win the person's trust. In this regard, a social engineer might choose to play the role of a customer service representative to get enough information to invade someone's computer. For instance, when a client calls a cashier in a bank to inquire about some vital information, the cashier might want to know some verification details, such as the account name, the account number and even the social security number (Jacquith, 2007: 67). When the client gives this information, they expect to receive service in return. Suppose this information is given to a cyber attacker posing as a cashier, and then this information is given to the hackers without the knowledge of the customer. This means that, through social engineering, hackers exploit loopholes to obtain the information they want. Thus, most of these types of attacker are former employees who have left the company with lots of bitterness.

These individuals can also develop malware which they use to harm computers in the same way that other hackers can. Indeed, worms, Trojans and viruses are some of the malwares used by attackers to commit cyber crimes. For instance, when attackers plant worms in a victim's computer, they use the computer's own system resources to the extent that its speed reduces. In addition to slowing down, the invaded computer can show pop-up error messages even when the system is not in use (Johnson, 2013; Opala & Rahman, 2013). However, the worst thing with these malwares is that they replicate and multiply to such an extent that they can do serious damage to an infected computer. In addition, when

they have multiplied to high enough levels they are capable of erasing the computer's files, and thereby the cyber terrorist succeeds. If this happens to financial institutes, this could lead to loss of money, which might affect the national economy.

Along with Trojans, viruses and worms, the cyber attackers can use botnet attacks. According to Opala & Rahman (2013), a botnet is a computer that has been set up to relay or transfer information to a main system; the information to be transferred can vary from personal information to financial or highly confidential information. However, most of the botnet attacks take place without the host's knowledge. In addition, they mostly take place at home, because home computer users hardly ever install firewalls on their computers. Moreover, home users hardly ever take security measures to protect themselves and their computers from cyber attack. This is due to the fact that security products are expensive, and usually bring added complexity to home users, who are not experts in dealing with security incidents. In contrast, big companies buy licenses which, when used appropriately, can protect their employees from malicious invasion. Home users often assume that, because they are not connected to large companies, they are thus hardly part of the hackers' plans (Grow, Elgin & Herbst, 2006). Once the bot is inside the computer, the attackers can use a root kit to manipulate the data in the system as well as maintain access to the invaded computer (Grow et al., 2006). To do this, the hackers conceal their presence by erasing log activity and the system log. In addition, the development of a house automation solution that allows multiple appliances to be connected to the Internet so that the user can control it remotely raises new threats, where hackers can hack into such appliances and use them for malicious purposes.

Click fraud has also been used by hackers, though as a less intrusive attack. According to Grow et al. (2006), click fraud happens when a person clicks an advertisement or a banner, so that the click rate for that advert is significantly increased. Thus, this happens even when the person doing the clicking is not interested in the particular advertisement – its statistics increase nevertheless. Similarly, experienced hackers use auto click software or automated programs to run some websites. A good example is the case of the California hacker who was arrested for threatening Google, Inc. with releasing self-made click fraud software (Muller, 2008). The companies that use click fraud benefit from the ads over the Internet in unjust fashion, which encourages malpractice; thus, it is considered a legal issue.

Spam, on the other hand, is when attackers flood the Internet or email address of the victim with numerous copies of the same message (Georgala, Kosmopoulos, & Paliouras, 2014). They send these messages to people who would otherwise have not chosen to receive such messages. However, users think this method of attack is less harmful, since they only see junk files of messages and advertisements in their address books. The spammers identify a few email addresses from which they start their attack, and in the process extend their invasion.

Another method the attackers will often use is Denial of Service (DoS). This method does not take confidential or sensitive information from the victim but only attempts to annoy the user. This is

because through the denial of service, the hackers are able to stop the user from accessing services on the system. The DoS can be very devastating to the victim, since they can crash his or her services. In this regard, DoS attacks are considered more similar to program exploitation than network-based exploitation (Adams, 1990: 299). However, for hackers to benefit through this method, they must take advantage of poor vendor implementation.

Hackers can also use the phishing method, which attempts to manipulate victims to voluntarily give out the information that is crucial to the invasion. Through phishing, users are manipulated into handing information to a person or site that are not known to them. The con artists often improve or refine their phishing ideas. Today, since most people are aware of such bad intent, they have changed their target audience and instead trick only a selected group of persons. Mitnick & Simon (2002: 59) describe this form of phishing as 'spear phishing', since the hacker attacks a selected group of persons. Thus, they only attack individuals who the attackers are convinced are on a certain mailing list, or who belong to a specific bank. To persuade their victims, the hackers use sites that look trustworthy to the users, and in the process lure them to enter their personal information, which they later use for their own benefit.

Therefore, hackers often exploit three computer security issues. To start with, hackers often take advantage of the vulnerability weaknesses which enable them to reduce systems' information insurance (Erickson, 2008: 109). Thus, through vulnerability the attacker identifies a flaw, accesses the flaw and exploits the accessed flaw. However, an attacker can only do this by using the tools and techniques which are required to connect to a system (Beaver, 2011: 66). On the other hand, the attackers benefit from exploits such as spoofing, Escalation of privilege (EoP), Denial of service (DoS), pivoting, Trojans, worms and viruses, which are able to take advantage of vulnerabilities, glitches and debugs. In addition, attackers who rely on DoS gain control of a user's computer and thereby hinder them from accessing services.

This section has clearly identified how cyber attackers conduct their malicious activities, and it is obvious that cyber criminals employ active methods to achieve their objectives. This confers an asymmetric advantage on the criminal. At the same time, victims of these cyber attacks are restricted to passive defence, which is not sufficient to defeat cyber attackers' active methods.

2.1.4 Types of Malware

Researchers have identified 10 types of malware, and brief descriptions are given below.

Figure 2.1: Types of Malware (Source: Author)

Table 2.1: Types and Description of Malware

Type	Description
Spyware	Hackers secretly install spyware on a computer system to collect and send information about computer usage as well as other personal and confidential data to its developer. The spyware infects computers through deceptive ways, which include Internet add-ons or plugins, free online scanning, search engines, dubious websites and even images (Squidoo, 2012).
Worms	Infectious and self-replicating, worms spread by either exploiting vulnerabilities on the target system or by using some form of social engineering to trick computer or system users into executing them. They utilise computer networks to send replicas of themselves to connecting computers on those networks (Kent et al., 2005). They pose a major threat to large computer networks (CISCO, 2012).
Adware	Adware is advertisement-supported software, and designed to display advertisements on computer systems and websites, or to send advertisement emails. Some types also act as spies to steal users' sensitive information (Squidoo, 2012).
Trojan horses	Trojan horses normally pose as a type of a free, useful software or add-on, but once installed gives hackers access to the system for performing their criminal operations from a remote station (Ken et al., 2005). Once a Trojan is activated on a host computer, server or network, it can cause a number of attacks, which include damaging the host by activating and spreading other malware, stealing data, deleting files, changing desktops and/or installing pop-up windows (CISCO, 2012).
Crimeware	Crimeware is developed specifically to carry out crime on the Internet, especially to steal financial and confidential information such as credit card data and passwords that can be used to access private online financial services identities or bank accounts. It is usually installed through social engineering, or

	by duping Internet users to release their confidential information (Squidoo, 2012).
Hijackers	Hijackers modify the browser settings of a user's computer to redirect it to the page of the developer's choice. Usually the user is directed to start pages as well as search pages with paid advertising. Sometimes hijackers may cause the browser to crash or the computer to run slow (Baratz, 2004).
Keyloggers	Keyloggers are created to monitor user keystrokes so that the information is logged and reported to the developer or the person/organisation that installed them. They are used as spyware to steal users' identities and confidential information. They can also be used by organisations to monitor employee activities (Squidoo, 2012).
Logic bombs/slag codes	A logic bomb is "a computer instruction that codes for a malicious act when certain criteria are met", which could include a particular action like deletion of a file or a program timed to run at a specified time in the computer's internal clock. In this case, the logic bomb waits until a specified time or date to log its destructive payload. It normally exists by itself, without having to replicate itself; and to complicate the code even more it can be attached as a genuine file (Robillard, 2004).
Dialers	These are programs that set up modems to connect to a 1-900 number, thereby enabling the developer or owner of the program to acquire revenue at the expense of the original user. Once they are installed in the computer, they change the user's modem access numbers to some especially high-cost access numbers, normally in another country (Baratz, 2004).
Viruses	Viruses can get into the system embedded in a software program. They can disrupt the activities logbook, replicate themselves, and increase the workload of the machine (Squidoo, 2012).

Figure 2.1 and Table 2.1 explain the types of malware used by cyber attackers and how resourceful they are in allowing attackers to achieve their criminal objectives. Cyber criminals use these malwares for many purposes. Most of the time, they are used as intelligence-gathering platforms from which to perform their malicious activities against other targets, and as sources for stealing money. It is clear that these malwares are active in nature, and used successfully against targets that rely on passive security controls. Therefore, current passive security controls are not sufficient to beat cyber attackers' active methods. Due to this fact, defenders need to change their methods of defending their assets, and think of ways to use similar techniques in order to succeed against cyber criminal actions, as the active methods used by cyber attackers are very resourceful. If the defender gathers intelligence from the attacker's domain, so the defender's cyber SA will be enhanced, and will be more accurate in predicting attack, as the SA will be built based on intelligence from two domains, rather than from a single domain.

2.1.5 Categories of Malware

There are three major categories of malware, observes Clarke (2009): Vector, Payload and Invocation. The first of them, Vector, enters a system through copying from a portable storage device plugged into or directly connected to the computer or system, or through downloads from another device on a remote network or a local area network. Vector-malware classified downloads or transmissions include those that infect a computer or system through file transfer using software that executes a standard protocol, which could be FTP, or a proprietary protocol, as long as the protocol is implemented on both devices. They also include malware transferred through malicious emails, the web, bulletin boards,

instant messaging systems and P2P networks. A Trojan is an example of vector download malware (Sinha, Kemerlis, Pappas, Sethumadhavan, & Keromytis, 2014).

Second, Payload malware is active code usually delivered to the target device so as to perform the function of its sender (or developer) or hacker, although it may perform other functions than its ultimate purpose. These include obscuring its existence or operation. The scope of this malware normally excludes the code that causes it to replicate itself (Alcorn, Frichot, & Orru, 2014).. As such, payloads have applications which are able to perform any operation on data. These applications are able to create data by inserting data into control files, inserting entries into the computer's or system's list of executable programs whenever the device is starting up or shutting down, deleting data or directory entries, modifying data by changing security settings for user-accounts or files, and modifying parameter-settings and port-settings (Sinha, Kemerlis, Pappas, Sethumadhavan, & Keromytis, 2014). Payloads also perform data capture and data disclosure by performing the functions of spyware, keystroke loggers, Trojan horses and adware, as well as including malware that can operate or act on software by installing malicious software, and making modifications to software to establish a new backdoor which allows the hacker or developer to gain access to user-accounts on a computer or system by bypassing safeguards and install a rootkit that obscures the operations of the malware. Payloads also modify anti-malware software to reduce its effectiveness. They can also modify malware that already exists on the computer/system to enable them operate without detection (Clarke, 2009).

Third, Invocation malware is used to cause the code to run into the target computer/system. Invocation comprises codes which are native to the instruction-set of the target computer/system, those that require an interpreter or run-time interpreter or compiler, and those that require embedded codes such as macros on spreadsheets and word-processing documents (Alcorn, Frichot, & Orru, 2014). Invocation malware is capable of causing malware to run in the target device remotely through a website application attack, a user-account or a bot, or by action of a remote device, where a bot is malware that can be triggered remotely so as to perform a specific function (Clarke, 2009: 22).

The above summary states clearly the active methods used by cyber attackers and their advantages in taking control over targeted systems. Therefore, defenders can also use these methods to protect the CNI and prevail over cyber attackers. Cyber SA can rely on these active methods to enhance the intelligence and thus the perception of the situation, so that defenders can be a step ahead by monitoring attackers' activities both from the attacker's and defender's domains (Peterson, 2013). This new intelligence-gathering capability is required, and offensive, active methods must be utilised by defenders in order to achieve an organisation's security goals.

2.1.6 Categories of Cyberwar

In their article 'Countering Cyber War in 2011', the Carnegie Mellon University Computer Emergency Response Team (CERT) divided cyber warfare into three categories: gaining information superiority; limited cyber war and unrestricted cyber war. While the first level is an extension of the commonplace

military goal of gaining advantage by virtue of information, the second level involves damaging the civilian Internet infrastructure. The third level is tantamount to a third degree of attack, since it aims to completely destroy the social fabric of a nation by causing maximum damage to civilian infrastructures such as emergency services, aviation control, the stock exchange and power generation systems (Shimeall, Williams & Dunlevy, 2001). Therefore, from a strategic perspective, the current state of cyber threat relates to Critical Infrastructure Protection (CIP), such as aviation (Gorman, 2009), finance (Wagner, 2010), water (Preimesberger, 2006) and electricity (Meserve, 2007), besides social and political situations (Orr, 2007), since all of them are currently connected to the Internet.

2.1.7 Sun Tzu's Military Philosophy

The above state of affairs clearly shows that cyberspace has become a new warfare domain that is spread across the globe via computer networks, where its intangible nature makes it difficult to assume the location of any possible zone of attack. Such a situation influences cyber operators to find ways to successfully manage their cyber systems, which in turn influences them to learn tactics from military strategists, such as Clausewitz (Western view, kinetic-non-kinetic warfare) and Sun Tzu (Eastern view, yin-yang warfare), where Clausewitz's (1976) principles follow a Newtonian view of the world and Sun Tzu's principles emanate from the concept of deception.

Clausewitz (1976) conceptualises war by using objectives, plans and other principles for attaining political objectives. According to him, war is a type of politics which served well both citizens and strategy makers in the post-Napoleon era. However, Clausewitz found it difficult to tackle irregular wars, since Western warfare did not experience such situations frequently. On the other hand, Sun Tzu focuses on using the intelligence of one party to defeat the other. His strategy involves the concept of yin and yang in Taoist philosophy, which is better suited to cyber situations since it covers all possible situations, especially where the issue of intelligence is involved. For example, the integration of networks takes place in the mind of the commander, which includes cyber support and the intelligence fusion centre. By deception in cyberspace, the mind of the commander can be attacked (Cahanin, 2011; Nakashima, 2010; Thomas, 2009). It is clear that from the military perspective of defence, intelligence is at the heart of establishing SA, and that most of the time this is achieved by being active behind enemy lines. Without intelligence, one will be battling with inferior SA (i.e. partially blind). Therefore, this argument can also be applied in cyber space, where a cyber defender should actively collect intelligence from behind enemy lines so that complete intelligence can be provided to help build the active SA.

The 2500-year-old Sun Tzu's military stratagem propagated in the book *The Art of War* (Sun Tzu, 1994), prescribes using deception, adaptability and speed as the mother of warfare strategies. Besides that, he suggests making the enemy's communication systems the primary target, stressing the importance of tactical reconnaissance, observation and flank patrolling, and considering probing attacks to be as important as battle itself. In his view, moral strength and intellectual prowess prove decisive factors in any long-term strategy.

Sun Tzu defends his military strategy with strong arguments. For example, he states that it is only the enlightened ruler and the wise general who will use the highest level of intelligence in support of the army for purposes of spying, and thereby achieve great results. Cahanin (2011: 1) states that such "focus on the criticality of intelligence, deception to defeat the mind of the enemy, and knowing that relationships between things matter most in the strategy of war" make Sun Tzu's philosophy an important guide to successfully managing cyber war. Many researchers highlight the striking resemblance of the 13 ideas of Sun Tzu and modern cyber war situations:

Table 2.2: Cyber Interpretation of Sun Tzu's Strategy

Tactical Suggestions of Sun Tzu	Cyber Situations
AoW I: Laying Plans	Good leaders not only exploit flawed plans, but also exploit flawed adversaries (Parks & Duggan, 2001; Sawyer, 1994).
AoW II: Waging War	After stealing the credentials and privileges of an authorised user, the hackers become insiders of the system and cause further damage by fulfilling their mission, such as creating DoS or espionage (Addinall, 2012; Geers 2011).
AoW III: Attack by Stratagem	In case the fight involves IT infrastructure, a cyber-only victory is the only way to protect the same, and for that matter it is important to attain victory before combat is even necessary (Sawyer, 1994).
AoW IV: Tactical Dispositions	The primary challenge in cyber warfare is to know whether the system is under attack, and therefore the short-term cyber defence goal is to improve an organisation's ability to collect, evaluate and transmit digital evidence (Geers, 2011).
AoW V: Energy	Both attackers and defenders try to outrun their opponent in terms of application (Geers, 2011).
AoW VI: Weak and Strong Points	Adversarial cyber reconnaissance should be difficult and confusing to the attacker so that they doubt whether the information they get is accurate (Sawyer 1994).
AoW: VII: Manoeuvring	Cyberwar simulates strategic bombing submarine warfare, special operations forces, and assassinations (Parks & Duggan, 2001), where hoodwinking the enemy through misinformation plays a big role (Addinal, 2004; Yuill, Denning & Feer, 2006).
AoW: VIII. Variation in Tactics	Commanders should not rely on the good intentions of others or count on best-case scenarios (Sawyer, 1994). In cyberspace, computers are attacked from the moment they connect to the Internet (Skoudis, 2005).
AoW IX: The Army on the March	Much like in real-time war, cyber commanders also need to check all nuances of the system while counter attacking the enemy, and should always remember that the attacker can also apply deception (Sawyer, 1994).
AoW X: Terrain	Cyberspace contains more dangers than the real world, since terrestrial distance does not play any role while one is connected to the network. Cyber weapons, too, are unreliable in character, since they are prone to reverse engineering. Thus it takes meticulous pre-operational cyber attack planning and timely application to manage cyber terrain (Parks & Duggan, 2001).
AoW XI: Nine Situations	Dispersive ground; facile ground; contentious ground; open ground; ground of intersecting highways; serious ground; difficult ground; hemmed-in ground; desperate ground (Sun Tzu, 1994). The cyber operators must fight both in their own and in the attacker's territories, and in the process such situations can occur anytime (Sawyer, 1994).
AoW XII: The Attack by Fire	The cyber operators need to accomplish something for which DoS appears ideal, i.e., to sever communications between enemy camps

	(Geers, 2011).
AoW XIII: The Use of Spies	IT security requires broader organisational support to maintain the critical infrastructures, and for this it needs to analyse the cyber environment by deploying spies. For example, pro-Palestinian hackers denied service to around 700 Israeli domains during the 2006 war between Israel and Gaza (Stoil & Goldstein, 2006).

The above points altogether highlight the fact that Sun Tzu's Eastern world philosophy conceptualises war by focusing on the criticality of intelligence, the use of deception to defeat the mind of the enemy, and the knowledge that relationships between things matter most in the strategy of war (Cahanin, 2011). According to this view, cyber deception has already been proved to be a potent weapon against the attackers, whereby it enables the operator to hide the real situation from the attacker and instead present a make-believe situation (Masip, Garriodo & Herrero, 2004). In spite of this development, a move toward using deception to enhance cyber SA, it is still not sufficient, as further active components should be considered in order to be able to collect intelligence from the enemy's domain, as that is what active SA requires so the new proposed model will correctly aligned with doctrine.

2.1.8 Counter Initiatives

The malicious codes that are known as computer worms, malware or viruses first surfaced in 1949 with the advent of self-replicating automata proposed by John von Neumann. Although such codes remained at an experimental stage until the early 1990s (Chen & Robert, 2004), in that decade the cyber world witnessed an explosion of malware both in terms of number and potency, which influenced network-savvy countries to indulge in serious research. For example, DARPA (the US Defence Advanced Research Projects Agency) was formed in 1958, which analysed five characteristics of worm: (i) discovering the target; (ii) ways of transmission; (iii) activating the code; (iv) managing payload; and (v) motivation of the attacker. DARPA finally conceptualised Internet worms in terms of attacker motivation (Geers, 2011: 23), as Table 2.3 shows.

Table 2.3: Correlation between Attacker's Motivation and Types of Worm (Geers, 2011)

Attacker's Motivation	Name of the Worm
Experimental curiosity	Morris/ILoveYou
Non-existent or non-functional payload	Morris/Slammer
Backdoor creation for remote control	Code Red II
HTML proxy, spam relay, phishing	Sobig
DoS	Code Red/Yaha
Distributed DoS	Stacheldraht
Criminal data collection, espionage	SirCam
Data damage	Chernobyl/Klez
Political protest	Yaha

While the above table shows that the range of computer hacking can extend as far as the hackers can stretch their imagination, the researchers established the following issues that have both broadened and deepened cyber security problem space:

- System vulnerability due to high cost of producing quality software

- Technical challenges involved in software patch deployment
- Susceptibility of the common C/C++ languages
- Usage of administrator rights by common system and programs
- Pursuing monoculture computing environment (Geers, 2011: 23) (Ransome & Misra, 2013).

The reliability of the above information is supported by the fact that Kaspersky Lab identified 42,250 unique samples of malware in a single month, May 2009 (Geers, 2011). From the above table, the current point of interest regarding malware revolves around Stuxnet and Flame, where the former is a highly sophisticated malware discovered by one Belarusian anti-virus firm in 2010, and which was used to destroy a Iranian uranium centrifuge in 2010 (Devine, 2010); the latter was discovered during an investigation that was prompted by the International Communication Union (Bitdefender Labs, 2012; GMA News 2012). According to Kaplan (2012), Flame is the most powerful and sophisticated cyber weapon ever to be developed, while the researchers at the Kaspersky Lab reported that Flame is 20 times the size of Stuxnet, and far more powerful (Kaspersky Lab, 2012). Its main purpose is to perform cyber espionage by stealing information from systems and computers that it has already accessed. Therefore, more sophisticated cyber attacks require more sophisticated means of cyber defence against them i.e.means that are more capable of producing more sophisticated cyber SA. Since the two players in this situation are using different methods, this puts attackers in a better situation, and so the defenders should start to change their passive defence approach and adopt a more offensive and active approach so that they can defend themselves better.

2.1.9 Current Combat Tools in Cyber War

As a result of the increase in sophistication of cyber attack activities and organisations, and the defensive methods they use, we must acknowledge the current asymmetry between cyber attackers and defenders. Adoption of a guarded active defence approach is already in place under the label of ethical hacking and use of honeypots. So, the world is already seeing active paradigms for Computer Network Defence (CND), in spite of the legal constraints imposed. This section will cover the aspect of cyber deception, and how this technique can be adopted by a defender to enhance its cyber SA and cyber security while controlling the effects of cyber attack.

2.1.9.1 The art of cyber deception in cyber security

The connotation of deception in cyber parlance can be explained by saying that cyber deception is all about hiding the reality from the receiver of signals in order to gain certain benefits (Masip, Garrido & Herrero, 2004). While this is applicable to both ethical and unethical hackers, ethical hackers can secure moral support for their deception, such as claiming that they need to remain covert in order to protect the safety of a network from cyber attack. Therefore, deception, from the perspective of ethical hackers, can be a great tool for a much-required hassle-free cyber operation. From the above perspective, all cyber operators or commanders need to play the role of ethical hacker, and therefore they too need to master the art of cyber deception to foster cyber security. So, through this approach, defenders will be able to gather intelligence from cyber attackers, which eventually will help to build

an enhanced cyber SA, as intelligence from such methods generate more reliable data as the sources the domains owned by attackers.

Cyber deception involves imitation and dissimulation, which can be achieved by deploying several methods. Rowe & Rothstein (2004) present a comprehensive list of the same, along with observed ratings regarding their suitability for offensive and defensive cyber operations, as shown in Table 2.4.

Table 2.4: Deception Methods and their Utility Value in Cyber Operations [Rowe & Rothstein (2004: 24)]

Deception method	Suitability for offense in information systems, with general example	Suitability for defense in information systems, with general example
supertype	6 (pretend attack is something else)	0
whole	8 (conceal attack in a common sequence of commands)	0
agent	4 (pretend attacker is legitimate user or is standard software)	0
object	8 (attack unexpected software or feature of a system)	5 (camouflage key targets or make them look unimportant, or disguise software as different software)
instrument	7 (attack with a surprising tool)	0
accompaniment	9 (a Trojan horse installed on a system)	6 (software with a Trojan horse that is sent to attacker)
location-from	5 (attack from a surprise site)	2 (try to frighten attacker with false messages from authorities)
location-to	3 (attack an unexpected site or port if there are any)	6 (transfer control to a safer machine, as on a honeynet)
location-through	3 (attack through another site)	0
direction	2 (attack backward to site of a user)	4 (transfer Trojan horses back to attacker)
frequency	10 (swamp a resource with tasks)	8 (swamp attacker with messages or requests)
time-at	5 (put false times in event records)	2 (associate false times with files)
time-through	1 (delay during attack to make it look as if attack was aborted)	8 (delay in processing commands)
cause	1 (doesn't matter much)	9 (lie that you can't do something, or do something not asked for)
effect	3 (lie as to what a command does)	10 (lie as to what a command did)
precondition	5 (give impossible commands)	8 (give false excuses for being unable to do something)
ability	2 (pretend to be an inept attacker or have inept attack tools)	5 (pretend to be an inept defender or have easy-to-subvert software)
content	6 (redefine executables; give false file-type information)	7 (redefine executables; give false file-type information)
measure	5 (send data too large to easily handle)	7 (send data too large or requests too hard to attacker)
value	3 (give arguments to commands that have unexpected consequences)	9 (systematically misunderstand attacker commands)

It is understandable that the above methods can work both ways, i.e. in favour of both ethical and non-ethical hackers. For example, an unethical hacker could provide a fake webpage to lure innocent visitors with the aim of earning money, and can influence them to lose it, while an ethical hacker can use the same mimicking technique to hoodwink an attacker for purposes of protecting his/her network. When this method is used by ethical hackers, intelligence about attackers is easily gathered so that the defender can understand the intention and motive behind the cyber attack. Also, such intelligence will

help to identify the method used by attackers so that better security can be adopted. Such information is very important, because this intelligence will help defenders to build better SA about cyber incidents, which will eventually lead to better cyber security.

Here, one can argue that it is not easy to deceive Internet users in this Information Age, where there is plenty of knowledge available regarding how to detect and avoid cyber deception. Yet, cyber deception has become a global concern, mostly due to two facts: one, computer users have a tendency to believe what they see before their eyes, and therefore are somewhat gullible to well-organised cyber traps (Rowe & Rothstein, 2004) (Poursaberi, Yanushkevich, Gavrilova, Shmerko, & Wang, 2013); two, such tendencies emanate from the novelty of the medium, which influences the perceptions of users, a situation which is explained in McLuhan's (1964) famous theory that the medium is the message, which shows that humans once displayed the same credulous attitude when newspapers were novel and themselves acted as messages, or when radio was novel and did the same.

Thus the hackers capitalise on such human vulnerability. Consequently, websites that want to do real business suffer from incessant cyber attacks, as they are the favourite targets of hackers, since many websites have weaknesses at one or the other of their layers, and it is easy to navigate the sites that are open for all (Barber, 2001).

The increasing instances of cyber crime strongly demonstrate the fact that the cyber world has become the number one crime zone – more so than the real world. For example, US organisations alone incurred $100 billion losses every year due to cybercrime and cyberespionage, according to a report published by the FBI. This in turn shows that factors such as the ease of committing crime – often within a few minutes – the easy availability of 'crime instruments' (hacking tools), the easy availability of huge number of 'soft targets' in one single place, and the ease of operating from home, have together contributed to the huge boom in cyber crime (Gorman, 2013) (Grazioli & Jarvenpaa, 2003).

Unethical hackers are also exploiting various ways to improve their techniques, since that is all they need to invest in. On the other hand, ethical hackers are desperately seeking ways to conduct vigorous tests to measure the effectiveness of all the protection tools that are employed in cyber protection management.

It is interesting to note that it is human error that has been found to be one of the most significant sources of susceptibility in any secure information system. In a survey done in 2006, it was found that about 60% of security breaches were connected to human error made by security managers and other information professionals. Not only that: the research findings also found that cyber crime had not only engulfed private and public organisations, but also had become a nightmare for ordinary people, who had become dependent on online activity for financial or other information exchange. Complaints from common people are now literally pouring in regarding Internet fraud. For instance, the FBI recorded a 33% increase in individual cyber crime complaints in 2008 than the volume it received in 2007. At the

same time, it also found an amount as startling as $264.6 million had been siphoned from ordinary people (Zyda, Spraragen & Ranganathan, 2009).

Such a state of affairs thus fully legitimises the deceptive operations of the ethical hackers, who actually work towards uncovering unethical hackers and preventing them from looting organisations and individuals. However, the power balance clearly favours the unethical hackers (Geers, 2011), as they solely focus on the destructive aspect of technology. It is for this relentless counter-research of the hackers that decoys, honeypots and other anti-hacking programs are being used, but they are yet to become fully effective. Websites employing systems to deceive intruders and prevent unauthorised access to their sites, such as tar traps (Hollinger, 1998), are also falling short of optimum performance.

Computer systems, too, are vulnerable to attacks, which in turn supports the need for wider application of deception for protection. However, the concept of deception by defenders is still in its early stages, at least in the general cyber world. There are calls for taking help from the military sector, which utilises a variety of deception techniques to successfully defend its networks. Nonetheless, not all measures and strategies have analogues in cyberspace. Some of the most pertinent examples are honeypots which decoy computer systems that encourage attacks with the aim of collecting data and information about the attackers and their attack methods so that better cyber SA and cyber security can be put in place. In this respect, researchers advise employing deception tactics, such as identity deception, false delays, fake information and false error messages (Bayuk 2011).

As mentioned earlier, it is difficult to defend against cyber attacks and crimes, since the practice is asymmetric, with the advantage in the hands of the attacker, who usually remains in a position to decide on the place, time and method of attack, about which the defender cannot gather any clue beforehand. This gives the attacker a better chance to perpetrate the crime. Such a state of affairs thus shows that there is an urgent need to devise a multi-layered defence mechanism which would be able to detect and handle the attacks in an effective manner. It goes without saying that there should be a concerted effort to defeat the cyber attackers, and with this in mind operators should explore all possible avenues to effectively beat the attackers in all phases of the attack process. The attack process is generally composed of the following steps, although it slightly differs from one network professional to another: reconnaissance; scanning; obtaining access; retaining access; covering tracks; and hiding (Kjaerland, 2005).

In addition, the support of the law is also essential in fighting cyber crime; hence, there should be legal cooperation among states regarding the enforcement of agreed standards of cyber conduct. For that matter, all states should reach a consensus on the forms of conduct that should be regarded as cyber crime within national borders, and the same then should be interpreted into a legal regime wherein those states should strictly forbid the identified forms of destructive cyber conduct and at the sometime set a framework to share cyber incident intelligence so all states collaborate in fighting cyber crime (Lobel, 2012). Since unethical hackers always exploit any easy access to information, there should also

be an effective defensive architecture in place to identify the real intention of each cyber visitor, so as to filter the cyber criminals from ordinary people (Hansman & Hunt, 2005). This research found that cyber deception is an essential component of cyber security for gathering intelligence about cyber attacks, helping build a strong cyber SA; thus, cyber deception is required for active cyber SA. There is a plethora of literature that deals with the art of cyber deception in cyber security, the topic of this study, which will be covered in the discussion section.

From the research and review of the literature from various authors and scholars, much can be discovered with respect to the topic of study. However, this section calls for providing certain basic information regarding the efficacy of ethical deception (deception employed by an ethical hacker) in protecting the networks in form of active defence that deploy such active measurement for cyber security. For example, ethical deception can be an effective instrument for cyber operators to use to collect information that valuable to security agents, who in turn could catch the cyber criminals by devising better strategies. One important point emerges at this juncture: that there should be a clear guideline to seize trans-continental cyber criminals; and it is high time the governments of various states open a clear dialogue in this regard. It is the absence of a universal policy to frame cyber space that is providing huge advantage to the cyber criminals (Nomikos, 2005).

Cyber deception can also be used as a perfect shield to protect any organisation's data and information critical for its operation. Therefore, from a business perspective it can be said that cyber deception can also be a source of competitive advantage to the business organisation, as it can facilitate efficient operations for them. A classic example of the same can be found in the instance of Coca Cola's cyber operation, as no one has been able to steal its business information, such as the ingredients it uses to manufacture Coca Cola products, which in turn provides the company with competitive advantage (McCarty, 2003).

2.1.9.2 The role of cyber deception in cyber security and defence

Confidently, there are instances that suggest gradual development in practicing deception to beef up computer security against cyber attacks. For example, there is increased use of encryption, which is a form of deception security measure used to hide information by deploying confusing strings of random symbols (Rowe & Rothstein, 2004: 34). Randomisation has already been identified as an essential tool for preventing hackers from obtaining information that can enable them to exploit the victim's system behaviour (Masip & Garido, 2004: 25). The use of honeypots, another security measure based on deception, is also on the rise. Honeypots attract hackers by impersonating different machines that are worthy of being attacked. In spite of these efforts, the role of deception still remains mostly under-utilised, and opportunities where defensive deception could have been useful are often missed. In any case, researchers have already provided a number of deception taxonomies that can be used to keep hackers at bay. Deception is a crucial resource for active SA, to allow defenders to gather intelligence and understand the enemy's intentions and methods. This will eventually help the defender make better decisions.

Deception consists of simulation and dissimulation, where simulation is known as showing false information, which is essential in launching a defensive attack against the hackers. On the other hand, dissimulation is used as an offensive attack by enabling the user to hide real information from the attackers. Dissimulation aims to exploit three offensive techniques, which are masking, repackaging and dazzling. The masking technique enhances dissimulation by blending a relevant object with the background and making it seem irrelevant so as to escape detection. For instance, "a malicious JavaScript may be embedded as a white space in a relatively benign looking JavaScript. In addition, an important private text message may be embedded as a white font in the whitespace of an apparently innocuous email message sent to a group" (McQueen & Boyer, 2009: 2). The repackaging technique works by hiding the real object, where it makes a relevant object appear like something which it is not. This technique is applied to phishing attacks by exploiting friendly, official and innocuous subject lines to propel a receiver to open the message. Finally, the dazzling technique hides the real object by making the relevant object seem very confusing due to giving adverse information about its true nature (Masip & Garrido, 2004: 41).

In deception, the obfuscation and randomisation of identifying elements are essential methods for inducing confusion. For instance, in an encrypted channel the meaning of the message remains hidden while making it clear and obvious that a message was sent. In every deception there must be dissimilation and simulation, since it requires some kind of false display to completely hide the real elements. In this regard, simulation plays an important role, as it contains three effective techniques, which are *invention*, *mimicking* and *decoying.* Invention is a creative form of deception, which develops a perception about the existence of a relevant object, when in reality there is no such object. For instance, a honeypot might be used in a system to give the appearance of a subnet of machines, and where such a subnet of machines displays exact IP addresses, when in actual fact there is no such subnet (Burgeon & Buller, 1994: 161). Similarly, mimicking creates misinformation by displaying characteristics of a relevant and actual object. Phishing attacks are a good example of the same, which may direct the hackers to a web page that appears to be a valid page of a reputed firm (Whaley, 1982: 188).

However, decoying, the third form of simulation, is the most interesting, as here the falsehood is displayed to turn the attention of the hackers from more relevant objects to the displayed, false object. For instance, when a web page with false but realistic data is used to attract a hacker's attention, this deception helps keep the hackers away from the real data.

Altogether there are seven security dimensions in a cyber security control system, which are security group knowledge, attack group knowledge, access, vulnerabilities, damage potential, detection and recovery (Whaley, 1982: 191). These dimensions play a critical role in creating the foundation for defensive actions (Burgeon & Buller, 1994: 178). Massip & Garrido (2004: 41) observe that these seven dimensions of security can be defended by the six deception types. For example, deception can

prevent the attackers from accessing the mechanisms and processes involved in security systems (Masip & Garrido, 2004: 42), whereas deception techniques such as "randomization system diagnostic and the timing of audits to reduce predictability could make it very difficult for the potential attackers to defeat the security control mechanisms" (McQueen & Boyer, 2009: 4).

This shows that deception can beat the hackers if it can successfully play its role in creating a false perception of the object and hiding the real object from attack, which would limit the attackers' knowledge of the real object (Rowe & Rothstein, 2004: 39). So, cyber SA can learn from attackers in order to deny the purpose of their cyber attack. Often, masking proves to be the best deception technique to prevent attack of this dimension of security, as it prevents leaking of information. Alongside it, techniques such as inventing, mimicking, repackaging, dazzling and decoying can be used to confuse the hackers (Rowe & Rothstein, 2004: 41). SA must have the variety to match the complex environment it seeks to protect against adaptive attacks, a variety which can be achieved through utilisation of deception.

Deception also plays an important role in preventing the attackers from accessing the information on the other security dimensions. For example, the six dimension techniques which make the actual information appear different to the hackers than its true nature can mislead the hackers. In this way, the operators can successfully hide the information regarding vulnerabilities, access and damage potential of the network by using deception (Burgeon & Buller, 1994: 179).

Another good way to prevent hacker interference is to minimise the number of accessible security services, which can be done by using the six deception techniques, including masking and repackaging. Alongside these, dazzling can be employed by randomising the IP ports and addresses, since the presence of many ports and false traffic can mislead the attacker. The following table shows how deception techniques can be used improve the security of the access dimension (McQueen & Boyer, 2009: 6).

Table 2.5: Deception Types and their Utility [adapted from McQueen & Boyer (2009: 6)]

Types of Deception	Defensive Actions
Dissimulation	Defence that hide services from the attacker.
Masking	Masking is any method that prevents attackers from observing services associated with the control system. • Configure to not answer pings. • Configure firewalls to prevent traffic flow between the control system and external networks, except as required. • Hide control systems communications from external network behind a NAT (Network Address Translation device).
Repackaging	Repackaging hides service information by making the service appear to be something that is of no interest to attackers. • Running a service on a non-standard port. • Providing service connect headers, which make the service appear to be another, more secure, version of the same service, e.g. make Wu-FTP appear to be ProFTP.
Dazzling	Dazzling can be used to hide information about the system services by making what is observable by attackers confusing or unintelligible. • Encryption should be used for all services when feasible. • Randomisation of IP addresses.
Dissimulation	Defence that hide services from the attacker.
Inventing	Inventing is any deception that causes the attacker to falsely see services that do not exist. • False network traffic that contains IP addresses and ports that do not exist.
Mimicking	Mimicking can deceive the attacker into believing that a relatively unimportant service is a critical component of the control system. • If there are multiple versions of the same service, make them all appear to be the same version on the same machine.
Decoying	Decoying is a diversion meant to divert the attacker's attention away from critical aspects of the control system network. • False network traffic that leads the attacker to phony, seemingly vulnerable services located in virtual machines.

Table 2.5 summarises different techniques of cyber deception, but it is important to understand that, in order to enhance cyber SA and be able to defend actively, it is crucial to know that these deception techniques alone are not sufficient. However, knowing how to plan and execute these deception types requires military strategic thinking in order to get the full advantage out of it, so that strong cyber intelligence can be gathered, better cyber SA can be achieved and effective defence can be put in place against cyber attack.

2.1.10 The Crucial Role of Offensive Hacking in Cyber Security

The traditional, reactive approach to cyber security is increasingly becoming insufficient before the increased dynamism of the cyber world, since it works with past knowledge and does not have the capability to exploit the vulnerabilities of the attackers. On the other hand, the offensive method of ethical hacking works its way through the vulnerabilities of the attackers, thereby providing greater scope for web commanders to protect their own sites. The offensive hacking method essentially comprises deception, which works as "an important two-agent psychological phenomenon with many applications to information security" (Rowe, 2004: 1), such as is used by an offensive agent when attackers try to hoodwink the information systems into providing secrets or destroying themselves, while occurring as a defensive screen by feigning an exaggerated processing delay to create a make-believe situation for the attackers to believe that the computer has succumbed to a DoS attack and so move away. This shows how an offensive method can fulfil the old adage that prevention is better than cure.

However, it is not that the attackers do not know about such strategies; therefore, they can reappear with a new style of attack, which requires that defenders apply new strategies of deception to outwit the attackers' prowess. According to Bell & Whaley (1991), the operator can adopt at least six deception tactics to protect the network, which are masking, repackaging, dazzling, mimicking, inventing and decoying, while Whaley shows how nine types of misperception can be adopted to restrict the attackers, which are patterns, players, intentions, pay-offs, place, time, strength, style and channels. There are other concepts, too, which show that the offensive method has a huge role in protecting the network, even though such techniques are still detectable due to fact that current deception uses low levels of interaction which can be detected, so attackers will find new ways to defeat it.

The scope of SA requires intelligence from outside one's own network to be able to find essential elements of information about attackers. The currently adopted SA relies only on intelligence that comes from one's own network, which is incomplete, as information about what an enemy is hiding or wants to hide is not acquired. This can be overcome by developing a theory and practice of active SA that adopts deception and offensive measures to build cyber SA. It worth to note that active defence must include target acquisition in the process of information gathering (ISTAR: Intelligence, Surveillance, Target acquisition and reconnaissance). Benign software, (Benware) that has no intention of manipulating the normal execution of the target. Unlike malignant software, the purpose of such software is to cause damages in the target. Therefore, Benware is a Trojan based software used by defenders with an intention to gather intelligence from enemy in the form of self-defence.

In addition, deception is dependent on enemy vulnerability, and therefore the operator should exploit a program that is capable of outwitting the attackers' perceptions about the state of the targeted network, as well as the attackers' perceptions of what they gained in the end. For example, one typical program, called Benware (a tool used by defenders with no intention to leave damages in the targeted host where

Malware as discussed earlier has an effect such as destroy, deny, degrade etc.), can be used to achieve such a successful result against the attackers in the following manner:

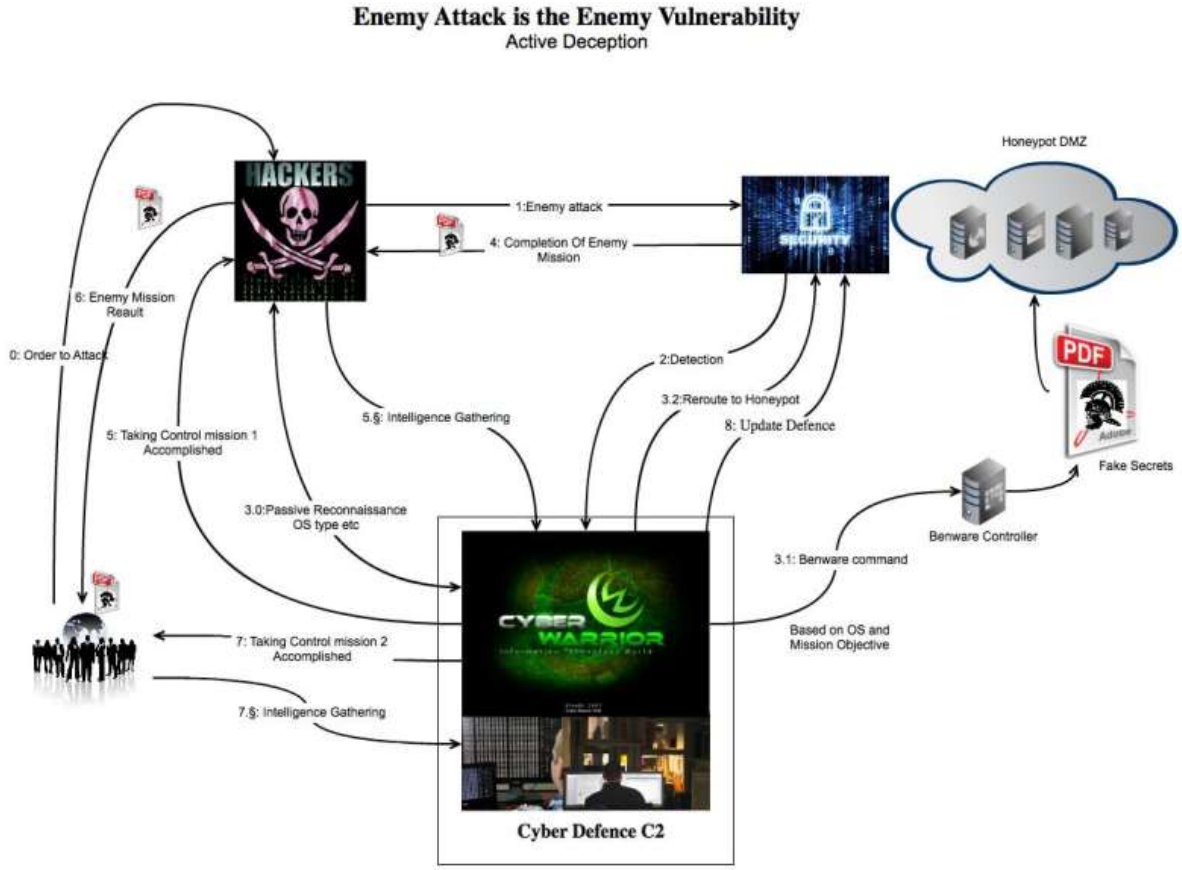


Figure 2.2: Exploiting the Benware Program to Deceive Attackers (Source: Author)

Benware is a Trojan-based program that can be used by a defender to gather intelligence from an enemy domain or network. This program requires the utilisation of active, offensive hacking and deception techniques in order to be executed and transmitted into an enemy network. Through this, an Active SA can be established.

Figure 2.2 highlights how the Benware (Trojan) controller contributes to the entire process of deceiving the attacker through using commands prepared on the basis of the OS and the mission objective of the operator, where in the end the attacker has to remain unknowingly content with fake secrets/intelligence.

2.2 Situational Awareness Research Initiatives

2.2.0 Governments and Cyberspace

The growing instances of state-sponsored cyber espionage programs have become a serious concern for maintaining inter-country relationships. Many countries are gearing up for global cyber war, which could be more devastating than what the world witnessed in earlier world wars (Gorman, 2013). Already there are several instances of cyber attacks led by the security agencies of various

governments, which have paralyzed civic life and business transactions, caused damaged to infrastructures, and spread panic among common people. For example, stung by the attack of the Stuxnet cyber worm virus in its secretive nuclear facilities in 2010, Iran became actively engaged in cyber warfare through its 'Iranian Cyber Army' (Rudner, 2013).

Cyber attacks are mostly unique in nature, and there are innumerable ways they can strike. It is becoming increasingly difficult to 'defend' computer systems with the 'known' knowledge bank, and accordingly, the old adage 'prevention is better than cure' is gradually influencing countries to take the offensive against any invader in their systems for the sake of protection. Therefore, this offensive stance also requires changes in the way SA is developed. Therefore, active defence and active SA will help in reducing cyber uncertainty and at the same time provide better risk management.

2.2.1 Government Initiatives to Develop Cyber Attack Power

The fact that countries across the globe are apprehensive of cyber attacks becomes evident from their own governmental documents. For example, in January 2013, PLA's (China) Lieutenant General Qi Jianguo openly commented in the official weekly newspaper of the Chinese Communist Party Central party school that "The West's so-called 'Internet freedom' actually is a type of cyber-hegemony", besides stating that "seizing and maintaining superiority in cyberspace is now more important in this information era than seizing command of sea and command of the air" (Bellacqua & Hartnett, 2013). In addition the cyber commons underpins all the commons; namely: air, maritime (sea), space and land.

Jianguo's comments, however, avoided the issue of their own cyber attacks, which has recently been exposed by an investigation conducted by the US private sector. The investigation published a report called the 'Mandiant Report', which went into detail on how one of the cyber-espionage units of the PLA had been hacking into the *New York Times*' computer systems from 2012 to mid-2013 (Feakin, 2013).

Instances like the ones cited above thus prompted the US government to draw up a list of potential overseas targets for US cyber attacks in a project named 'Offensive Cyber Effects Operations' (OCEO), which clearly suggests that the US government is stepping up its cyber offensive capabilities (Greenwald & MacAskill, 2013). This change in stance also requires changes in how SA is conceptualised and implemented in practice.

2.2.2 Inter-Country Cyber Warfare

The US and Israel have already been accused of masterminding the Stuxnet computer worm attack on Iranian uranium enrichment centrifuges (Greenwald & MacAskill, 2013), while Syria has openly deployed its 'Syrian Electronic Army', which is a hacker group engaged in bringing down, defacing or otherwise maligning sites that carry anti-Syrian government content. This group mainly targets media, as well as American President Barack Obama (Norman, 2011). China, on the other hand, has steadily been increasing its espionage network over the past few years. For example, SecureWorks, a leading

security services provider, reported in 2008 that it had recorded 7.7 million attempted attacks from China in that year. Not only that, China has also released a new hacking toolkit onto the market named 'Leopard in a Hole' that is priced between $20 to $500, which helps in penetration tests used to identify and exploit SQL injection flaws (Dwyer, 2009). This clearly shows how the world is moving towards more active methods in cyber space, so active defence is needed, and active SA is required to be able to tackle such innovative attacks.

2.2.3 Situational Awareness (SA) Theories and Models

Sun Tzu states that: "If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle" (Luzwick, 2000: 15). Therefore, intelligence is the secret to winning a war and nobody has attempt to determine a theoretical framework or measurement the effect of SA enhancement as a result of active SA which will be shown later in chapter 3.

The problem of uncertainty is that it is present everywhere, including all three phases of cyber situation awareness. The three phases of cyber situation awareness are prior security risk management, real time intrusion detection and posterior forensics analysis (Li et al., 2010, Eun & Abmann, 2014). When we talk about real time situation awareness, the invisibility of cyber attackers increases due to the degree of uncertainty in the cyber world. It is near impossible to find out where the cyber attackers are located, when and how the cyber attackers are going to commit a crime. IDS sensors are available, but they can only halt the symptomatic phenomena of the attacks, and there is no guarantee whether the attack has taken place and whether the cyber attackers have succeeded or not (Eun & Abmann, 2014, Li et al., 2010). This section presents an overview of Situational Awareness (SA) and how it can be used to respond enemy attacks in cyber space, as well as pointing out the current limitations; plus specifying the gap where new capacities for cyber SA are required.

In literal terms, situational awareness means to acquire knowledge about the things going on around us (Adams et al., 1995; Endsley & Garland, 2000). The term 'Situational Awareness' itself is an area of research although the concept has a long history behind it (Harrald & Jefferson, 2007). SA can be traced back to the theory of the military grouping with the NCW (Alberts, 2002). Quite extensive research work took place in military aviation security in the mid-1980s for the purpose of designing computer boundaries for individual operators (Endsley, 1988, 1995; NASA, 2006).

Cyber Situation Awareness, usually referred to as Cyber SA, is still considered to be an area of research that is always evolving in an increasingly interconnected age, which made its mark with Denning's (1987, 2001) pioneering work on using expert systems to detect computer attacks in 1987. That was followed by a plethora of experiments covering areas such as anomaly detection, pattern matching, agent-based systems etc, which are now described within the confines of level 0 or early level 1 data fusion (Salerno et al., 2008; Tadda, 2006, 2008).

The early stages of these experiments shaped the concept of tactical fusion, which was proposed by the JDL (Joint Director's Laboratory) model in 1992, and which gained popularity among researchers. This model contains five functional levels, 0, 1, 2, 3, and 4. It was published by Hall & Llinas (1997), and it focuses solely on data management for preventing cyber attacks. Here, most of the tasks are concentrated on levels 0, 1 and 4. Tadda finds the JDL model to be a bottom-up, data-driven model (Figure 2.3). The significance of the JDL model lies in the fact that it highlighted the significance of algorithmic techniques in supporting situation awareness (Salerno, Hinman & Boulware, 2005).

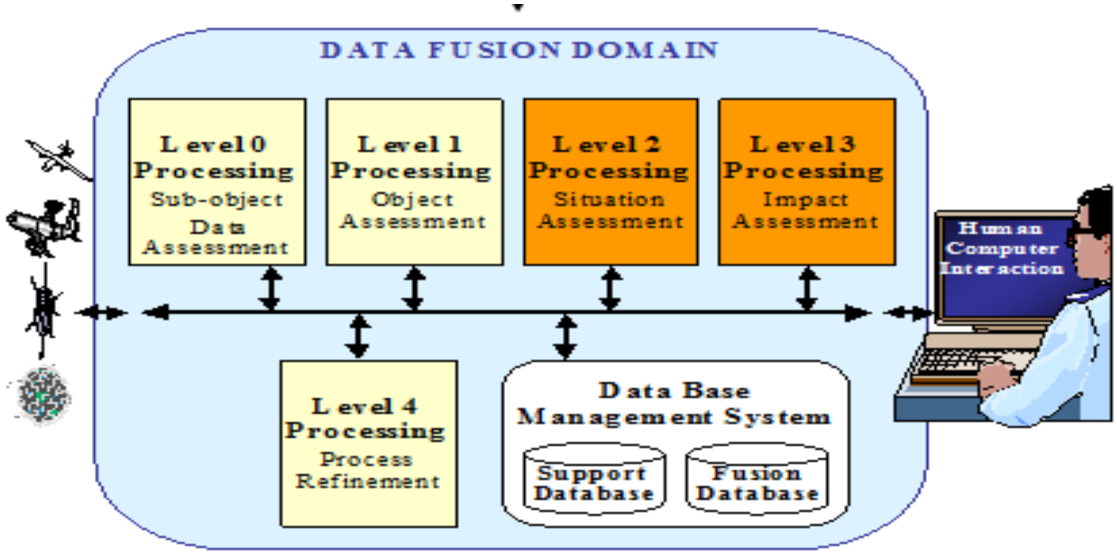


Figure 2.3: Tactical Fusion/JDL Model [adapted from Tadda (2008)]

However, the work on successfully comprehending the concept of SA was very much underway, since the researchers rightfully sensed that human elements are equally important in achieving quality SA. From a simple point of view, SA refers to knowledge about ongoing events in the cyber environment, but the three elements hidden in that definition – knowledge, ongoing events and the cyber environment – contain a plethora of elements that command human abilities, such as perceiving, comprehending and projecting the situation. In the wake of such requirements, Endsley (2000: 3) provided one of the briefest yet most comprehensive definitions of SA when she stated that SA refers to "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future".

This definition clearly underpins three essential drivers of SA, which are *perception*, *comprehension* and *projection*. Endsley (2000) observes that the perception of cues (which she refers to as Level 1 SA) appears fundamental, since in the absence of basic perception of important information the chance of wrongly visualising the situation drastically increases. In support of her argument she cites a finding that that 76% of SA errors made by the pilots (either system failure or cognitive processing problems) stemmed from lack of perception of the required information (Jones & Endsley, 1996).

Comprehension, on the other hand, refers to an outcome relating to how people interpret, associate, store and retain information, and thus takes its place in the SA process at Level 2 SA in Endsley's (1995c) definition. Flach (1995: 3) argues that "the construct of situation awareness demands that the subjective interpretation (awareness) and in the sense of objective significance or importance (situation)". Equally, Jones and Endsley (1996) observe that lack of comprehension can cause 20% of SA errors.

The Level 3 SA, i.e. projection, helps operators to perform at the highest level of SA, since it enables them to forecast situational events and their dynamics, suggests Endsley (2000). Endsley argues that from an intuitive point of view SA is all about "knowing what is going on", while from a formal point of view it is all about "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 1995b: 36).

Thus, Endsley further consolidated the theoretical perspective of SA by adding human factors to it, thereby opening a new horizon of developments towards achieving quality SA (Wickens, 2008: 397). Endorsement of the above view from a host of researchers (Endsley, 1993, 1994; Endsley & Rodgers, 1994; Endsley & Robertson, 1996; Endsley et al., 1998) highlighted the temporal aspects, as the above view showed that both perception of time and temporal dynamics associated with events play crucial roles in the formulation of SA, and that a critical part of SA involves understanding the amount of time available in the occurrence of an event or in the course of an action. Such developments helped researchers to underpin time as an integral part of Level 2 (comprehension) and Level 3 (projection) SA.

Endsley (1995c) argues that the approach to earning quality SA should be goal-driven, since operators have multiple goals within any environment, which makes SA dependent on task performance and goals set in a specific environment. Smith & Hancock's (1995: 139) view that SA is "purposeful behaviour directed toward achieving a goal in a specific task environment" also supports Endsley's view.

Based on her theoretical understanding of SA, Endsley (1995a) developed her SA model, which is mostly referred to as a mental model comprising three levels: perception; comprehension; projection (Figure 2.4).

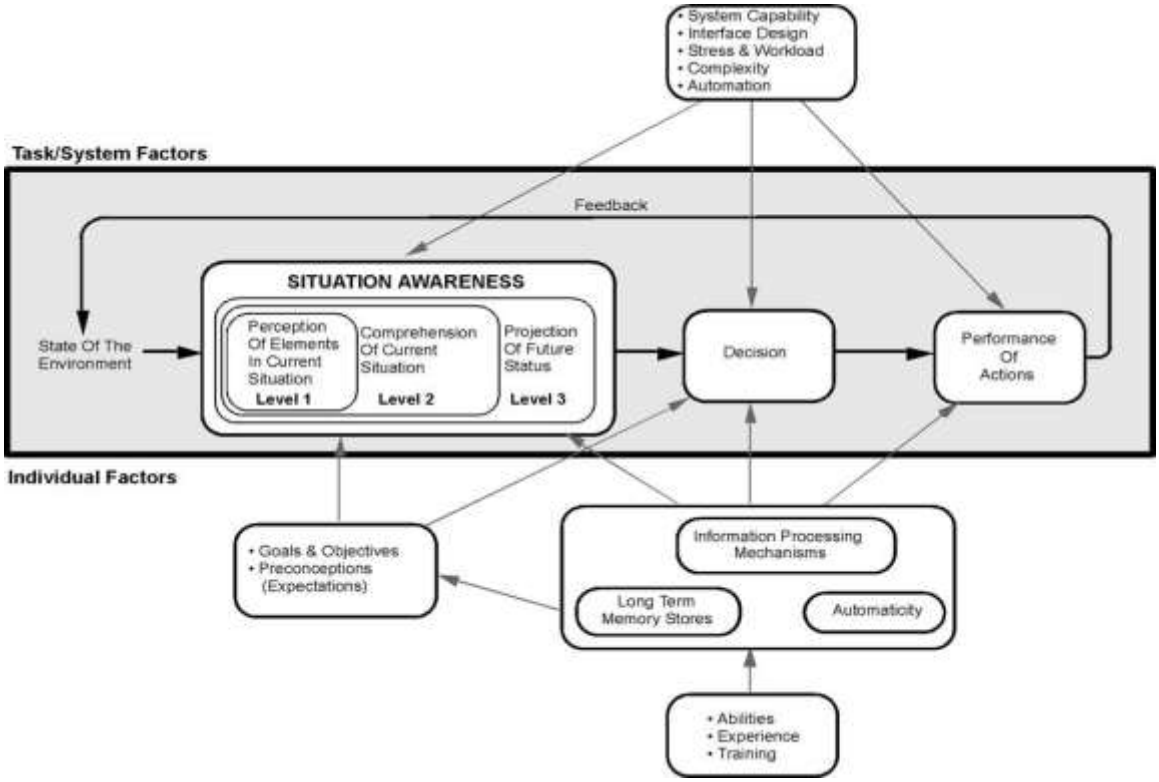


Figure 2.4: Endsley's Model (1995b)

The above model segregates SA from decision making and performance stages to depict it as an operator's mental model of the state of the environment, which acts as the main precursor to the decision making processes. According to Endsley (2000), the central tenet of cyber operation is to convert quality situation awareness into successful performance, which in turn requires treating SA as a separate stage of functioning. She defends her argument by saying that, while it is possible to obtain quality SA, it is not always possible to convert the same into action due to other intervening factors, such as poor strategy selection, lack of decision choices, technical constraints, lack of training and so on. With this she highlights the integral relationship between SA and decision making, where decisions are formed by SA in as much as SA is formed by decisions. From another perspective it can be said that this model depicts SA as a package containing both tacit and explicit knowledge (Nonaka, 1994; Nonaka & Nishiguchi, 2001), the successful exploitation of which depends on other appropriate external channels, such as technology, training and the amount of freedom available for decision making.

In the existing literature, SA is dominated by studies of individual operations and their dimensions (Stanton et al., 2001). You can find many separate and dedicated theories, such as Endsley's three-level model (Endsley, 1995), Smith & Hancock's perceptual cycle model (Smith & Hancock, 1995) and the activity theory model of Bedny & Meister (Bedny & Meister, 1999). In every model, the psychological approach, process and product are quite different. Take the example of Endley's three-level model. It is a purely cognitive theory which largely depends upon information flow and does not consider technological factors. Contrary to this, SA is described as a purely perceptual model by Smith & Hancock, and Bedny & Meister employ activity theory to explain SA. Ultimately, Endsley's model is

too general: it doesn't state how SA is achieved in detail, which makes it insufficient for cyber security. Also, the model was originally designed for pilot SA, and information about intelligence feed is not included in detail. The model is generally too abstract and high level, and detail on how SA is performed is not covered. Therefore, this model fails to address what is required to achieve SA, and fails to identify the domain of intelligence that basically is the source and the key to success in perceiving the situation.

2.2.3.1 Tadda's situation awareness reference model (combo model)

Tadda (2008), on the other hand, considers the JDL model as a Bottom-up, Data-driven and Functional model, considering Endsley's model to be a Top-down, Goal-driven and Mental model. He recognises the utility value of both, and accordingly proposes a combined model comprising the best elements of both, along with new elements such as an initial data requirement and textual input. In his model, Tadda begins by defining the problem/goal in a top-down manner, and then opts for a Processing Flow solution, by which actions take place such as projection (alerts), comprehension (model analysis), perception (data collection), parsing/extraction and data cleansing. At this stage, his model covers JDL's Level 0/1. Next, he opts for the task of Process Refinement, which deals with missing data, additional data and input for sensor management, before the model takes up the task of Off-line Processing, which involves knowledge discovery. Tadda's model is illustrated in Figure 2.5 below.

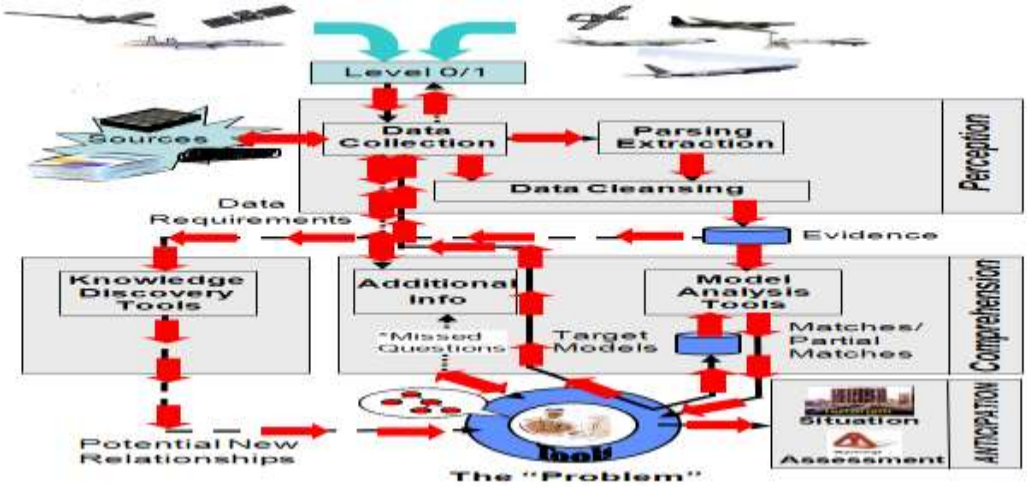


Figure 2.5: Tadda's Combination of JDL's & Endsley's Models (Tadda, 2008)

Tadda (2008) uses three broad areas of operation, being Anticipation, Comprehension, and Perception, and illustrates how this works when applied to the cyber SA:

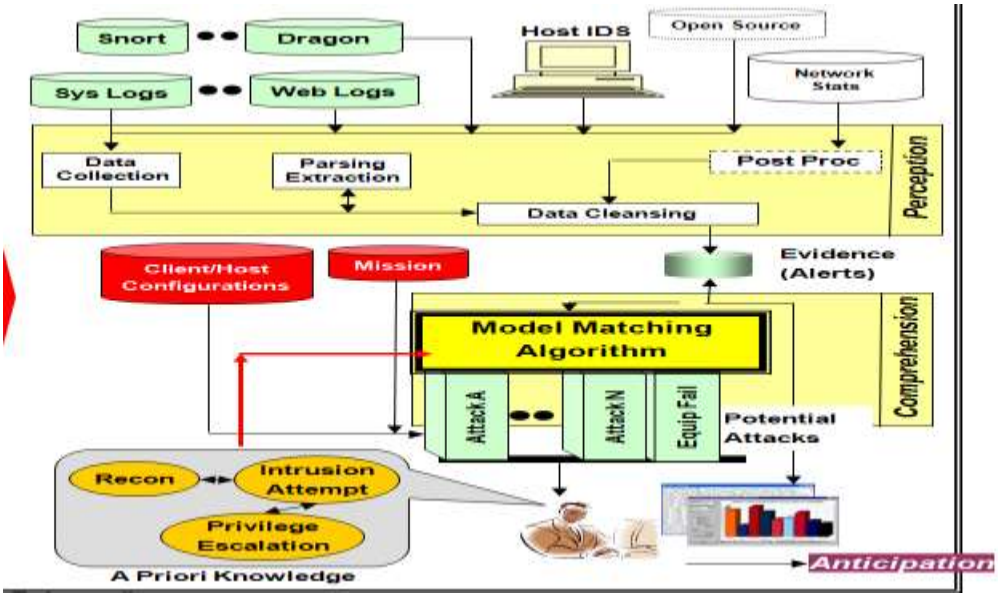


Figure 2.6: Tadda's (2008) SA Awareness Reference Model Applied to Cyber SA

Tadda (2008) suggests that this combo-model, applied to a cyber domain, would collect evidence at the Perception level, and then would comprehend the situation by recognising intrusion attempts and exploiting a priori knowledge, which in turn would enable it to anticipate the possible magnitude of impact. He illustrates the same through another diagram (Figure 2.7):

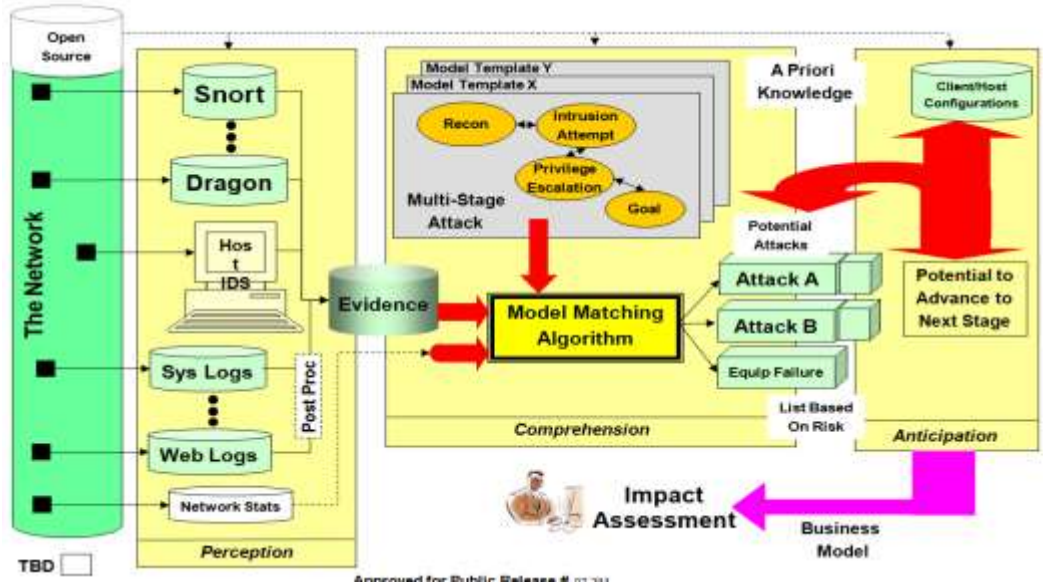


Figure 2.7: Tadda's (2008) Model Applied to the Cyber Domain

Tadda (2008) underpins seven variables as the main contributors to SA:

1. Evidence: Gathered through IDS alerts (Snort, Dragon), system logs, service logs (Apache and IIS) and network flow data;
2. Tracks: This refers to the collection of all evidence that are available against one or more targets made by one or more attackers;
3. Situation: This refers to the set of tracks at a snapshot of time;

4. Situation Awareness of a Network: This refers to the mental model of the analyst;
5. True Positive: This refers to a successful attack;
6. False Positive: This refers to an incorrectly identified attack;
7. Non-relevant Positive: This refers to the situation where the operators correctly identify an attack that has failed to penetrate.

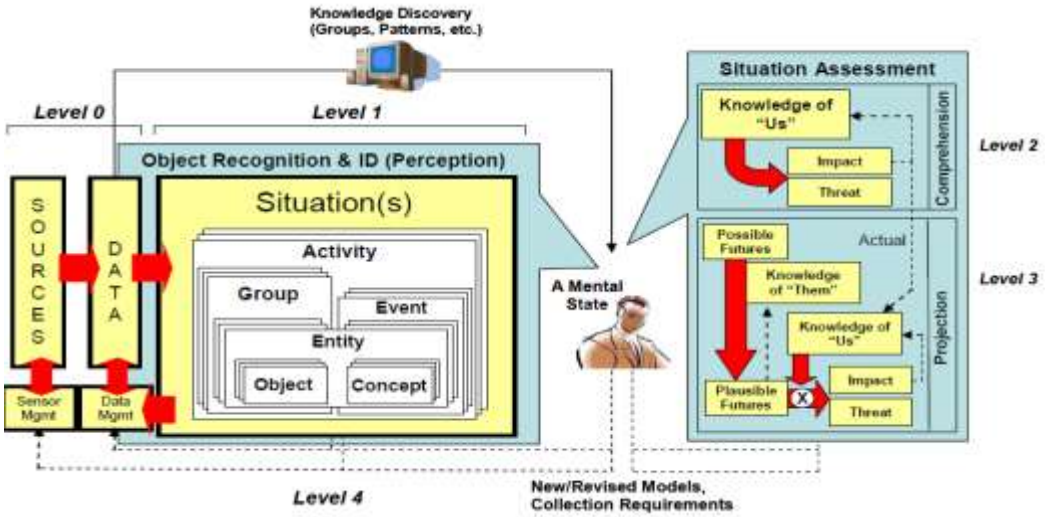


Figure 2.8: Revised Framework of SA Reference Model (Tadda 2008)

"The largest gap in current research is how to perform situation projection or anticipation – projection in the lower right section of the lower right section of the above diagram", observes Tadda (2008: 340), thereby underpinning the difficulty in determining possible futures, where it takes the 'knowledge of us' to combat the 'knowledge of them' (the attackers). This observation amply hints at the possibility that the knowledge of us at comprehension level 2 could fall short of meeting an actual situation in the desired manner if the attacker were to apply greater knowledge and skill. It also indicates that any scheme/model with a single goal of protecting against attack in a single domain environment always runs the risk of getting outwitted by an attacker with superior knowledge and skill. Interestingly, Endsley (2000) also speaks about the uncertainty involved in projection by stating that it is not always possible to convert SA into practice, identifying the quality of strategy as one of the main constraints. Another observation is that the Tadda model relies on data captured from local networks, which is not enough for cyber security as defence should look into data from cyberspace, i.e. other data that have effect in real life. Therefore, the Tadda model is focused on a single domain, and this makes the model passive, in turn producing incomplete SA. Cyber SA is not only about network data, but also must consider other effects on the environment of the cyber attack. Local monitoring of the network cannot detect zero day attacks, so zero day effects in the real world must be considered in order to defend against them better. Finally, the model neglects a very important source of intelligence which is crucial for cyber security: the enemy network. Without it, incomplete SA or poor SA will be produced. Therefore, the active SA model should consider this factor in order to enhance cyber security.

2.2.4 Intelligence and Situational Awareness

According to Peterson (2013), cyber security is one of the major concerns in the modern world. It affects everyone, including individuals, organisations, industries, and even government institutions. The reason why so many organisations are affected is because there is no proper structure for dealing with the cyber threats. Defence systems are insecure due to their design (Peterson, 2013). For this reason, there is an increased need for organisations to develop situational awareness on cyber security. This can only be realised through cyber intelligence as intelligence reduces risk and error propagation in decision making which eventually enhance cyber security. This part seeks to discuss, critically, the characteristics of cyber intelligence that can enhance situational awareness, as well as consider the approaches used in intelligence collection.

Intelligence operation can be defined as the act and process of gathering information about an enemy in order to uncover the enemy's motive and objectives. Intelligence operation is a multifaceted term that includes the following activities: direction and planning; data collection; data processing; data exploitation; data production and analysis; integration; dissemination; evaluation; and feedback (Prouty & Ventura, 2011). The process of intelligence operation can be daunting, and fraught with disappointments. Cyber SA, as explained earlier, needs to capture intelligence from multiple domains using proper methodology and plan if it is to uncover the enemy's intention and achieve better SA in a more comprehensive, timely and accurate manner.

2.2.4.1 Accuracy:

Accuracy of intelligence comes first in cyber security. Lehr & Pupillo (2009) indicate that accuracy of data assists in situational awareness in that it helps the organisation to take informed and certain steps towards cyber security. As Lehr & Pupillo (2009) note, the challenge in Internet security has persisted because there is no accurate information as to who propagates the attacks, when, or where they are initiated. Hu & Jiang (2012) indicate that the affected parties realise the need for accuracy in cyber security. As such, they organised a conference looking into measures aimed at improving the accuracy of such data. It is quite obvious why this accuracy is needed: ensuring cyber security is very important as it helps in safeguarding company secrets, identities and other sensitive information. Cyber security systems work based on the available information. Therefore, if the intelligence is not certain, organisations might invest a lot of money blindly, yet still suffer from the same fate they seek to evade. For this reason, it cannot be denied that accuracy of cyber intelligence is crucial for an organisation's situational awareness as quality SA requires high accurate intelligence and limited and inadequate intelligence will result I erroneous SA and propagation of error and uncertainty.

2.2.4.2 Timeliness:

In curbing the threat and avoiding excessive damage from any critical situation, timing is very important. Defensive intervention can sometimes come in too late, at a time when the damage has already occurred – a situation under which the effect of the intervention would be insignificant. The same applies to cyber intelligence. As Peterson (2013) observes, the perpetrators of the attacks keep on

devising new ways to carry out their attacks. This implies that unless there is timely intervention, then organisations will be forever prone to attacks. This calls for pro-active rather than reactive measures.

In order for the pro-active measures to be successful in controlling cyber crime, the collection of cyber intelligence must be very timely as well as accurate. Amin, Schwartz & Hussain (2003) indicate that cyber intelligence should be reliable in this way. That is, it must come in at the right time in order to prevent attacks from occurring. The importance of timeliness in situational awareness is that by observing it organisations can predict the next possible attack, the mode of attack or the areas vulnerable to attack. Consequently, measures can be put in place so as to make sure that actions are taken before it is too late. For this to be realised, the cyber security experts have to make proper preparations to deal with the attacks. This is where timely intelligence is needed. Failure of intelligence to have this characteristic means that an organisation will forever be going for curative measures rather than preventive measures. Timely intervention is the only solution, and this can only be facilitated by timely cyber intelligence which provides defenders the advantage of operating within the enemy's decision cycle and influence there action through utilising deception as discussed earlier. Active Cyber SA provides agility and can increase the tempo of the battle rhythm in cyberspace beyond the capabilities of the adversary i.e. out manoeuvre the enemy.

2.2.4.3 Completeness:

There is also the aspect of completeness. Organisations might have the intelligence gathered locally, but if it is incomplete then the organisation can be just as vulnerable as if it did not have any intelligence at all as this approach only look into one domain which is not adequate and that why active SA is required to overcome the issue of incomplete intelligence. The cyber security personnel would then be working with uncertainty, thereby providing a loophole, much to the advantage of cyber crime perpetrators. The issue of incomplete cyber intelligence is not new to organisations. GAO (2000) indicates that for a long time there were barriers to sharing cyber intelligence between affected players, i.e. government institutions and the private sector. As such, each had little bits of intelligence which were not substantial enough to make proper prevention measures. This is the reason why cyber insecurity has persisted. There are different pockets of intelligence, but still no way by which the dots can be connected in order to come up with a comprehensive security system.

There has also been a failure of the concerned parties to come up with comprehensive information. Bhaskar (2006) further indicates the damage caused by lack of complete intelligence. There is the absence of an adequate number of security officers trained in computer forensics. Therefore, Active SA requires proper training and a method to determine people performance. As such, even if the information is available, no one can fully make sense of it in order to devise a counter-measure. This is another issue that has greatly contributed to lack of completeness in cyber intelligence.

Due to the lack of completeness in intelligence, it is hard for organisations to make proper situational analysis. Thus, they are prone to continued attacks. However, GAO (2000) indicates that the affected parties realise the need for having complete intelligence. This is the reason why the barriers to sharing cyber intelligence are dissolving. Governments and the private sectors can come together and share the little information they have on the situation as indicated by UK government in CISPA (cyber intelligence sharing and protection act) (Lewis, Louvieris, Abbott, Clewley, & Jones, 2014). Through such measures, more information can be pooled to make meaningful conclusions. Based on this discussion, it cannot be denied that completeness of cyber intelligence is vital in ensuring organisations' situational awareness.

Much has been said about the intelligence. However, there is the need to look into the process by which this intelligence or data can be collected. Stevens (2012) indicates that the methods of intelligence collection are subject to criticism. As such, there is a need to look into why such criticism arises. This can be looked at in relation to the available approaches to intelligence collection. From the above discussion, the current methods of intelligence gathering is not sufficient to fight cyber attacks due to the reason covered earlier. Therefore, Active offensive intelligence gathering is required to enhance cyber SA and cyber security.

2.2.4.4 Passive data collection

Passive data collection is one of the approaches currently adopted in cyber SA models, as Tadda (2008) suggests: a data-gathering level from a local network without specifying details of what data are to be captured. Huey & Rosenberg (2004) argue that this provision was given under the Convention on Cybercrime (CC). Stevens (2012) further indicates that the Department of Homeland Security in the US asked for budgetary allocation meant for collection of computer and Internet data so as to enhance cyber security research. This approach is passive in nature because what is captured is only network data using technology similar to the one used at the organisational level, but this one is more like national level monitoring. Situational awareness is raised in this approach by employing monitoring data within their own network, which is again passive and incomplete as the defender can see only one side of the truth. Avenues that can be employed in this case include technological means such as network monitoring tools, firewalls, IPS, and IDS.

Passive data are invaluable in raising situational awareness for an organisation. Application of deep packet inspection gives an insight into the traffic content, thereby hinting at any suspicious moves. This arises through the identification of suspicious content. This also helps to reveal the Internet portal used in propagating the attack, as well as the possible impact of it (Holdaway, 2001). This can inform the organisation on the nature and urgency of the corrective action needed (Theohary & Collins, 2011). However, what the organisation sees in this case is valuable if it is to recover from a cyber attack, but it is not sufficient to deter the attack. This is because captured intelligence provides data about an incident already taking place, and gives insight into what attackers reveal about their attack, Therefore, cyber SA in this case is based on inadequate data, meaning that poor decisions will be made. Looking

into Endsley SA, intelligence issues in this case can lead to erroneous SA (Poor situation understanding, Poor judgment and Poor decision making).

2.2.4.5 Active data collection

This is where intelligence collection is not disguised. More often than not, this is carried out when an investigation is already ongoing. This can be through installation of physical data collection devices, as described by Chen, Tan, Xing, Wang & Fu (2012), through collaboration with Internet service providers (ISPs) (Huey & Rosenberg, 2004), or through utilising hacking techniques (Varon, 2002). Under such circumstances, organisations dealing with data are forced to collaborate with the security agencies. Ethical hacking occurs on a large scale during such activities, where government agencies can use it to gather more intelligence. Virus infection is another method that can be employed by intelligence services as an offensive approach. By introducing a virus, such as a law-enforcement Trojan, a government's intelligence services are able to discover their cyber enemies. This is achieved by noting those who try to terminate the government-powered virus (Chen, 2010). Such intelligence is important because it can help in ascertaining the origin of a given cyber attack. It can also be used in tracking cyber traffic; hence aiding in formulating measures and strategies that can help to improve cyber security (Theohary & Collins, 2011). Therefore, an active approach will provide more intelligence that can be compared with what is already seen in the passive approach, which eventually will aid in building proper cyber SA to deter cyber attacks. So, any cyber SA theory should take into account in enhancing cyber intelligence in order to enhance cyber security.

2.2.5 Collaboration and Sharing Cyber Intelligence

Current developments in information technology have been a major boost to the ways in which people conduct business. However, there is a challenge to associate equivalent developments with technological developments. There have been quite widespread incidents of cyber insecurity. Some of the unlawful activities committed through cyber crime include hacking, stealing of identities, stealing of copyrights and business secrets, cyber bullying and white-collar crime, such as fraud and embezzlement of funds (Ginovsky, 2012: 22).

These challenges have made the world in general realise that there is the need to act proactively and protect people from incidences of cyber attack (McGraw, 2013: 109). Cyber security has become a major security concern. According to White House.gov (2013: 1), cyber incidents are one of the major security challenges facing the US, to which no solution has been derived yet. According to Kaser (2012: 3), the US government decided on a Cyberspace Policy Review with three principal goals. First of all, it aimed to create a comprehensive line of defence to modern threats. Secondly, it sought to safeguard the nation from the full measure of the threats. Thirdly, it sought to protect the future of the cyberspace environment (House.gov, 2013: 2). This latter part stressed the importance of the primary goal: establishment of a front-line defence to face modern day threats. It aims to do this by asserting the fact that horizontal collaboration is needed, where organisations work hand in hand to curb this menace (Solansky & Beck, 2009: 852).

Solansky & Beck (2009: 830) indicate that cyber terrorism has become a major security challenge, matching up to other acts of terrorism. This threat does not only face the public; indeed, the private sector and investors are equal targets. Therefore, these actors are just as keen as the government to make sure that such crimes are prevented. Peterson (2013: 120) indicates that the vulnerability of the critical infrastructure in the US predisposes them to cyber attacks. This threat calls for the concerned parties to come together and form a robust group to counter this challenge. *The Economist* (2013: 61) posits that there have been several attempts to solve this problem. Among them is the Cyber Intelligence Sharing and Protection Act (CISPA). This is where the private sector and the UK government share cyber intelligence in order to help fight cyber crime. This calls for collaboration between the concerned parties as this bring down the of cyber security especially for SMEs (Lewis, Louvieris, Abbott, Clewley, & Jones, 2014).

Collaboration helps in gathering more information on cyber attack. House.gov (2013: 3) has it that when all the concerned parties bring to the table what little they have on cyber attacks, then it is possible to build a case on the notorious incidences, the frequency of their occurrence and the manner in which they are executed. With such information, it is possible to get into the minds of the perpetrators and predict their next move. This would help in countering them and curbing their activities. While this seems like a great idea for dealing with cyber security, it has to be noted that information sharing is not really as horizontal, as it should be. For instance, *The Economist* (2013: 62) argues that some cyber crime regulation measures involve regulation of networks. This has been done by the US Congress as well as the European Commission. Such occurrences cast doubt as to whether horizontal sharing can actually work. Some people feel that it is a move intended by the government to intrude into the private affairs of individuals (Albanesius, 2012: 1). This is the reason why the CISPA bill was so controversial, just like the SOPA bill, which sought to prevent online piracy. The argument is that through information sharing, people's private information would be freely accessible by the government (Kaser, 2012: 3), and that this would constitute an abuse of the Bill of Rights, whereby everyone is entitled to privacy.

House.gov (2013: 2) observes that sharing of information helps the concerned parties to deal with cyber threats. At this point, it has to be noted that cyber crime is quite elusive. As technology evolves, so does the nature and extent of the cyber crimes. As such, the methods derived by one party to deal with a given threat can soon become obsolete (Peterson, 2013: 123). As such, it can be quite time and resource consuming for one party to continually derive new methods of dealing with the incidents. This can be very uneconomical (Ginovsky, 2012: 25). However, when the parties come together and form a unity of purpose, they create a pool of information. Every party contributes intelligence gathered and the control methods they have derived. A combination of these strategies leads to the creation of a formidable force which can be used to crack down on the cyber terrorists. The US government has realised this, which is the reason why it came up with the policy of sharing information on cyber crime and cyber incidents. It is a way of building up a body of knowledge on this contemporary problem so

as to help all the concerned parties steer clear of the threats (Solansky & Beck, 2009: 860). Furthermore, House.gov (2013: 3) indicates that sharing of cyber intelligence is a strategy that can be used to get up to date, solid and reliable information on cyber situation awareness. This increased quality of information and awareness is important since it acts as a red flag for the organisations.

Again, this point seeks to prove that horizontal collaboration and sharing of cyber intelligence is the way to go. However, critics of the CISPA are of the opinion that this is just a strategy of the government to meddle in people's lives. Kaser (2012: 3) argues that the CISPA Act is just a masquerade by the government to enforce censorship and surveillance. The provisions seem to go against the rules concerning privacy, data security and cloud computing. This argument, however, is thwarted by Albanesius (2012b: 1), who indicates that some private companies realise the need for such collaboration. He gives the example of Facebook, which supported the bill, arguing that it acts as a bridge between the private sector and the government to team up and fight against a common foe. Therefore, all parties would benefit.

Another benefit from sharing of intelligence and collaborating in confronting cyber crime is that it helps in the construction of a strong cyber situational awareness, and so better protection for CNI. Everyone understands the potential threats, possible roots of attack and likely modes of attack (Albanesius, 2012b). As such, individuals, companies, states, firms and individuals know how to evade the pitfalls that can expose them to cyber attacks. Proper channels of reporting and dealing with cyber incidents are created, ensuring that no incidence goes unaddressed. Such a task force could be the key to saving a nation from the spectre of cyber crimes (McGraw, 2013: 121).

From a critical point of view, it can be argued that there are two major sides in relation to the CISPA and the Cyber Security Bill. On one side are the supporters, who argue that all concerned parties need to come together and work as one in order to counter the threat of cyber crime. The parties need to pull their resources together and create a robust team to curb cyber incidents in order to protect the nation's interests and resources (Solansky & Beck, 2009: 65). On the other side are those who argue that the bills are just disguises by the government, allowing them access to people's personal information. One undeniable fact is that such measures are needed to prevent cyber terrorism. Therefore, the parties need to find a common ground where they can work together for the good of all (Albanesius, 2012b: 2).

In conclusion, this section has highlighted the importance of collaboration and intelligence sharing for the prevention of cyber crime and cyber incidents. It has looked at the challenge of cyber crime and the efficacy of collaboration in dealing with it. From the discussion, it has emerged that cyber crime and terrorist incidents are major security challenges in the modern world. Such crimes are elusive because they continuously evolve over time, as technology evolves. For this reason, it would not be financially economical, and more time consuming, for a single entity to try and deal with the cyber attacks. Instead, the concerned parties should come together and form a union of purpose that can liberate them from this menace. Such a move would help in gathering meaningful intelligence on cyber crime, and

consequently help in the building a strong force that could effectively deal with the problem. Finally, the whole process would enhance an organisation's situational awareness, where resources and effort would be distributed among collaborating parties. This is a very cheap type of intelligence that cyber SA can use to learn and understand cyber incidents much better so that proper projections can be made. Therefore, Cyber Intelligence sharing is an essential dimension that must be incorporated in any cyber SA theory and model.

2.5.6 SA Agility

Albert & Hayes (2006) state: "SA agility is perhaps the most important attribute to SA approach" (57), and "the ability to recognize a need to change and the ability to adjust are associated with agility" (43), while pointing to the fact that agility is crucial for SA, since it ensures that the commander/operator remains alert enough to recognise the changes and to make necessary adjustments. In addition, they also make it clear that availability of appropriate resources, and the ability of utilising the same, contributes highly to agility. According to them, agility is composed of the following characteristics:

- Robustness – effectiveness across a range of tasks, situations and conditions;
- Resilience – the ability to rebound from damage or misfortune;
- Responsiveness – the ability to act within windows of opportunity;
- Innovation – the ability to do new things or old things in new ways;
- Flexibility – the ability to accomplish missions in multiple ways; and
- Adaptation – the ability to alter process and organization to improve effectiveness or efficiency.(Albert & Hayes, 2006: 189).

SA agility contains three independent variables, which are Timeliness, Adaptation and Responsiveness. Timeliness within this context covers several ideas, such as the availability of information relative to the time when it is needed, awareness attained relative to the time when it is needed, understanding achieved relative to the time when it is needed, the timing of a decision corresponding to the time when it is needed for action and timeliness of command intent (Albert & Hayes, 2006). The importance of timeliness in situational awareness is that through it organisations can predict the next possible attack, the mode of attack or the areas vulnerable to attack. Therefore, measures can be put in place so as to make sure that the appropriate actions are taken before it is too late. Intelligence's failure to have this characteristic means that an organisation will forever be going for curative measures, rather than preventive measures (Huerta, d' Entremont & González, 2006). Timely intervention can be the only solution, and this can only be facilitated by timely cyber intelligence.

Adaptability refers to the extent to which an SA model or approach can be modified in order to accommodate new developments (Saraswat, Pankaj & Rani, 2010: 555). As is well known, the world of IT is never a static one. On the contrary, there are developments coming in day after day. Similarly, attackers keep on changing their tactics. As such, an approach that might have been effective at a given time might soon become obsolete. At this point, it has to be noted that the costs and duration of the

process of coming up with an SA model is quite high. In order to ensure agility in SA, there is the need to have a flexible, dynamic model that can accommodate changes in the future (Saraswat, Pankaj & Rani, 2010: 555); as opposed to a static model, which cannot be altered. The latter would cost the implementing company a considerable amount. Therefore, it is arguable that a flexible model is more agile due to the fact that the flexible model will provide better agile intelligence, as it can be changed as per the developments in technology. It also remains active and relevant for longer.

Responsiveness refers to the ability to deal with fleeting opportunities available in all operating fields, such as in the tactical arena or at the operational and strategic levels. In addition, it refers to the ability to do new things, or to do old things in new ways (Huerta, d'Entremont & González, 2006). The significance of responsiveness lies on the fact that the pace of change has increased across the globe, while the adversaries have become more adept (Albert & Hayes, 2006).

2.2.7 SA Quality

SA quality provides the basis for agility, observe Albert & Hayes (2006), where the connotation of quality even covers the characteristics of SA agility. Apart from that, it is the quality of decisions, quality of planning and quality of execution that highly contributes to SA quality. Therefore, accuracy and reliability should be identified and put into consideration while building cyber Situational Awareness, as these two variables show how SA is being approached.

Accuracy of intelligence is vital in cyber security (Lehr & Pupillo, 2009). The persistence of the challenges in cyber security can be attributed to a lack of accurate information as to who prosecutes the attacks, when, or where they are initiated. Hu & Jiang (2012) indicate that there have been efforts to ensure this aspect of accuracy in intelligence. The concern for accuracy of intelligence resides on the fact that intelligence is vital in ensuring cyber security which, on the other hand, is very important as it helps in safeguarding company secrets, identities, and other sensitive information. The cyber security systems work based on the available information. Therefore, if the intelligence is not certain, organisations might invest a lot of money blindly, yet this suffers from the same fate they seek to evade. For this reason, it cannot be denied that accuracy of cyber intelligence is crucial for organisations' situational awareness.

There is also the aspect of Reliability. Even if organisations have all the intelligence needed, reliability is important to ensure that the information is actually helpful. Unreliable intelligence can mean that cyber security personnel work with uncertainty, thereby providing a loophole that can be exploited by cyber crime perpetrators. GAO (2000) indicates that, for a long time, reliability of intelligence has proven to be wanting mainly because there is no organised manner in which the intelligence can be gathered. On the contrary, different parties retain small pockets of information. As a result, most of them have certain amounts of information, but not in a comprehensive manner. This makes it hard to make any headway in dealing with cyber crime. To curb this situation and ensure reliability of information, Bhaskar (2006) indicates that there is the need for collaboration between the concerned

parties. This is the only way through which they can pool the information together and make sense of it. Otherwise, the current disintegration in intelligence renders the intelligence unreliable.

2.3 SELF-DEFENCE: LEGAL ASPECT

Cyber crime is a growing, global problem. Despite intense efforts by law enforcement officers to stop the practice, cyber crime continues to spread. Brenner (2010) says that, partly, the growth of cyber crime stems from the extra-territorial nature of the practice. On the contrary, Wall (2007) argues that the growth of cyber crime mainly stems from the changing nature of such crimes. The abuse of new technology has also led to the spread of this practice. Consequently, there have been rising numbers of cyber attacks in the United Kingdom and the United States. These countries have reported cyber crimes for many years, and, despite greater attempts to curb their spread, they continue to increase. Loader (2013) states that developing countries, which do not have established Internet networks, also report increased incidences of cyber crime.

The American government has treated cyber security with utmost importance. In fact, the US Homeland Security considers America as a breeding ground for cyber crimes. This is because America is not only a victim of such attacks, but also the source of most attacks (Schell, 2004) (Parish & Goostree, 2013). The Anti-Phishing Working Group produced statics that show the growth of cyber crimes within the past years (Chik, 2007). Increased awareness of cyber crime in the UK and America has largely driven the rise in the number of cyber crime litigation in both countries. However, most of these litigations do not have a common legislative basis.

This section explores the nature of cyber crime in the context of the laws of defence in the US and the UK, while seeking to find the legal background support the development of active cyber SA that relies on the offensive method as self-defence in cyber space to fight cyber attacks. In the subsequent sections the legal underpinnings of such laws are considered. Significant emphasis is made to compare the application of the laws of defence on cyber crime with the application of the same laws in the 'physical world'. In this regard, this section explores the laws of defence (as outlined by the UN), the right to bear arms, and the implications of these laws in cyberspace. This is because active defence and active SA have to deal with or operate within the constraints of a legal framework.

2.3.1 UK and US Laws on Cyber Crime

2.3.1.1 America

Since federal and state governments govern American states, the process of formulating laws is divided between the state and federal governments. Usually, state laws are more applicable to cyber crime, unless there is a special situation where there is a need for federal intervention (Chik, 2007). For example, when cyber crime threatens national security, federal cyber laws may apply. Alternatively, when the prevention of cyber crime requires the uniform application of law, the federal government may intervene in the formulation (or enforcement) of such laws. Therefore, because of the distributed functions of state and federal governments, both governments have historically contributed to the

formulation and enforcement of cyber law. Nonetheless, because of the political differences in America, every state formulates and enforces its own laws. There is therefore no legal requirement for all American states to adopt uniform laws (Chik, 2007).

There are also regulations which apply to jurisdiction in cyber protection. According to the Tallin Manual (2013), both the federal and state regulations apply within the territory of jurisdiction. As such, it is illegal for a state or the government to engage in activities that would lead to perforation of the cyber sovereignty of another nation or state, on whichever platform. Furthermore, rules apply that a state bears responsibility for cyber operations attributable to the said state. As such, the state would be answerable to any irregularity associated with cyber activities within its jurisdiction. Lachow (2013) notices that, despite the already existing regulations, there is a need for the US government to "provide greater clarity on which ACD actions are legal and which ones are not" (10). This is mainly because there are different approaches that the institutions might take in trying to curb cyber insecurity. Some of the options seem to be almost legal, while others are almost illegal. Clear guidance needs to be given on the same so as to avoid confusion.

2.3.1.2 UK

Specific legislations on cyber crime in Europe inform the UK's cyber laws. Indeed, there is a close relationship between Europe's public policy on self-defence and the UK's legislation on the same. For example, the UK is subject to cyber crime legislations, as formulated by the Council of Europe (CoE). Therefore, the provisions of self-defence laws (under the convention) are applicable in the UK, just as they are applicable in other European countries that are signatories to the convention. The close historical, geographic and economic relations between the UK and Europe inform the close interconnection between the UK's and Europe's cyber laws.

Nonetheless, the most common law governing cyber crime in the UK is the Computer Misuse Act of 1990 (Emm, 2012). The UK government has, however, updated this act with newer and stiffer penalties. The impetus to update this law came from the inadequacies of existing laws to curb hacking activities within the UK. Even more so, this issue came into sharp focus when previously existing legislations failed to convict Stephen Gold and Robert Schifreen for gaining unauthorised access to a UK organisation, BT Prestel services. Because of the inadequacy of the law to convict the two suspects, the court acquitted them (Emm, 2012).

The UK cyber laws also take an international perspective. A report by the House of Commons (2013) indicated that the UK recognises the actions of NATO as well as its international allies such as the US in dealing with cyber insecurity. The House of Commons sets out the regulations under which the Ministry of Defence (MoD) can implement cyber insecurity control measures without compromising the cyber sovereignty and integrity of other nations and partners. The report also stressed the fact that when dealing with cyber intelligence laws, the UK and its partners have to adhere to international standards such as those stipulated by NATO. It is clear enough that the current situation is still a grey

area. There are no clear laws allowing active defence, even though the UK's MoD can respond to cyber insecurity.

2.3.2 The Right of Defence

Normally, every country has a right to defend its people against any form of attack. However, technological advancements have introduced a new form of attack, which contravenes the conventional wisdom regarding the right to self-defence. Cyberspace is the platform where conventional rules of self-defence have been broken (Arsene, 2012). However, as Moore (2010) observes, several countries still adopt a conventional approach to preventing cyber attacks. For example, the US uses the military to defend the country against cyber attacks. Arsene (2012) questions the justification for doing so, because there are many risks associated with adopting a military approach to defending a country against cyber attacks. One risk is the overlap of self-defence and conventional-space defensive strategies. In other words, militarising cyber security may take a war-like approach, which should not be the case. Therefore, while conventional wisdom may approve the use of force in conventional space, use of force as a right to self-defence may not work in the cyber world. Therefore, even though a cyber attack may manifest the same characteristics as a conventional attack, responding to such an attack with force may be unlawful (Arsene, 2012).

People often compare the self-defence law to the English law. Researchers say this law is part of private defence because it allows for the use of illegal means to prevent an attack (or protect a country from harm) (Himma, 2008). In Britain, this law stems from common law and the Criminal Law Act of 1967 (Samaha, 2005). One common principle of self-defence rules focuses on the use of reasonable force to prevent an attack. Therefore, according to the nature of the law, self-defence is more of a justification than an excuse (Scheb, 2012: 417). Globally, the right of self-defence against cyber attacks is still an unresolved issue. Indeed, because of some of the complexities identified when comparing cyber attacks with conventional attacks, it is difficult for countries to exercise (blindly) their right to self-defence without considering the unique dynamics of cyber attacks (Committee on Deterring Cyber Attacks, 2010: 163).

The UK and the US share the same approach to cyber attacks. Both countries propose the use of force when cyber attacks result in death, injury, harm or destruction of property. However, the US has been most vocal about this provision. In fact, there are loud calls in the US to treat cyber attacks like 'ordinary' attacks if they cause death or property destruction (Committee on Deterring Cyber Attacks, 2010). The US Defence Department claims that it will not hesitate to use force to defend itself against cyber attacks that can kill, destroy property or harm its people.

2.3.2.1 The right of defence as per the UN law and proportionality of response

Article 2 (4) of the UN Charter describes situations when countries can use force for self-defence (Ellen, 2012). The clause discourages the use of force as a means to solve international conflicts, but it approves it when states need to defend themselves from external aggression. Article 51 of the UN

Charter stipulates this provision (Ellen, 2012). Many people have interpreted the provision of the charter as either supporting or opposing the use of force as a self-defence mechanism in cyberspace attacks (Jasper, 2012). Here, the main dilemma centres on whether to use force, even when there is no armed attack (such as in cyberspace). Some analysts have approved the use of force in such situations, while others reject the use of force (Ellen, 2012).

Because of the dilemma caused by the application of Article 51 (the use of force as a self-defence mechanism), the International Court of Justice has been forced to interpret the use of force as a self-defence mechanism. Milhorn (2007) explains the court's ruling by demonstrating that the use of force as a self-defence mechanism only applies to situations where there is a significant and real threat to a country. The charter also stipulates that the use of force only applies to the specific country that wants to defend itself (Ellen, 2012). Moreover, the article says that the intention to defend the country using force should show a high probability of success. Lastly, the charter says that the force applied should be proportional to the potential damage suffered from the attack (Schiller, 2010). However, in cyberspace, waiting for damage means acting in a passive way to the threat of cyber attack, whereas by taking an active approach this damage could be avoided through adopting a proper response to the cyber attacker.

All the above stipulations are difficult to apply in cyberspace. In fact, some observers say it is impossible to apply the above provisions to combat cyber crime (Wyler, 2005). Usually, complications arise when determining whether any direct loss of life (or any loss of property) meets the conditions for triggering article 51. Broadly speaking, it is often difficult to find the evidence that would trigger the activation of article 51.

The complications brought by the nature of cyber crime also pose a challenge to the implementation of article 51 of the UN charter because some cyber crimes are difficult to trace to one country. Moreover, even if a state traces the source of the attack to one country, they may not know the individual who is directing the attack (Wyler, 2005). For example, an attacker may infiltrate innocent servers and use them to direct the attacks, such as a zombie. However, it is true that sometimes attribution might be difficult to trace, but the utilisation of active defence and active SA are the ways to establish the source of attacks. Furthermore, trying to trace such attackers may consume a lot of time. Estonia and Iran provide examples of the difficulty of tracing attackers, because even though the countries experienced cyber attacks a few years back, they were still unable to discover the real identity of the attackers due to the fact that no active measures were in place, so both failed in the process of defence and identification of the attacker.

Lastly, the main issue affecting the use of force (as stipulated in article 51 of the UN charter) rests on the need to prove proportionality and necessity (Himma, 2008: 410). Apart from the time-consuming nature of attempting to uncover the identity of attackers, it is also difficult to prove that allowing a counter-attack may achieve the objective of preventing the attack. Similarly, it is difficult to limit the

effects on intended targets if a defensive attack occurs. According to the strict circumstances within which the UN allows defensive attacks, it is difficult to meet the criteria for launching an armed attack against cyber crime (Carr, 2011: 50). Therefore, even though cyber attacks may interfere with a country's economic sphere, air space, maritime space and/or territorial integrity, it is difficult to depend on article 51 of the UN charter to justify defensive attacks on cyber crimes. This issue is considered to have implications for the development of active cyber SA and active defence.

2.3.2.2. Right to bear arms

In the UK, the right to bear arms is part of English common law (Wyler, 2005). Scholars such as Aristotle and Machiavelli (Kates Jr, 1992) also recognised this right to be part of a person's right to self-defence. Similarly, the US constitution also acknowledges the right to bear arms as part of self-defence. The same protection is replicated in several state constitutions. Still in the US, the government introduced the right to bear arms as a Second Amendment to the Bill of Rights.

Parliamentary supremacy in the UK has, however, imposed many regulations governing the right to bear arms. For example, the prerogative to control the right to bear arms shifted from the monarch to parliament, of which the Pistol Act of 1903 was the main legislative provision (Wyler, 2005). The right to bear arms covers several weapons that are deemed offensive according to the law. Knives and firearms are the main weapons considered offensive by the UK law.

While the right to bear arms may be a critical part of self-defence law, its applicability in cyberspace is impractical. Indeed, the right to bear arms aims to protect a person from a physical assault (or harm). However, attacks in the cyber world are intangible but the effect in the real world is tangible. Similarly, as with other situations described in this thesis, it is difficult to know the attacker. Therefore, it is equally difficult to apply the right to bear arms as a means to protect a person from cyberspace attacks. However, since cyber attacks are getting more sophisticated, and cyber criminals are using active methods to attack, then the cyber self-defence law should be modified to allow active defence and active cyber SA.

2.3.3 Case Study and Discussion

Cyber space security poses unique challenges to the application of self-defence laws. For example, when two people share organisational resources through open port access, it is difficult to establish the legal justification for using self-defence legal provisions if an attacker tries to infiltrate the cyber network. This situation is true when one party gives another party the authority to gain access to the organisation's resources, where the second party responds to a security threat through the established connection. Technically, the second party would not be breaching the law because he/she is responding to the attacker through an established connection.

In the above situation, it is difficult to establish the right legal framework for approaching the issue, because the intention of the attacker is not established. If the second party knew the intention of the

attacker, it would be easier to justify the action of the second party who acts in self-defence. This scenario is played out in the Computer Misuse Act, which seeks to establish the intention of the attacker (first) before any legal consequences are determined. Without knowing the intention of the attacker, it is difficult to establish that the law has been broken. However, a hack is a hack, irrespective of intention. It is the behaviour which is illegal, and so in order to establish cyber self-defence, lawmakers should consider this behaviour in order to draw up the most suitable law.

An incident that occurred in the UK in 2004 demonstrates the need to establish the intention of the attacker before castigating that attacker. Here, an organisation accused a teenager of destroying a server by sending millions of mails to the server (Ellen, 2012). However, the court ruled that the defendant had not contravened the Computer Misuse Act because his actions did not lead to any unauthorised changes to the information on the computers. The failure to prove the intention of the defendant proved to be the biggest weakness here. However, if the organisation had been able to prove that the teenager had changed the information on their servers, they would have established the intention of the attack and held the defendant liable for his actions. However, they failed to do so.

The above case highlights the need to establish the intention of an attacker who tries to gain access to a cyber network. In the absence of a determined intention from the attacker, it is difficult to justify a response to an enemy threat. Therefore, the existence of the intention to gain unauthorised access to a cyber attack does not provide sufficient grounds to warrant a counter-attack. However, if the attacker were to go further and alter information on a server, there would be substantial grounds for a response – sufficient to warrant a conviction which may come late and not be sufficient in a case where the target is a national critical infrastructure.

Self-defence laws aim to protect people and organisations from injury or harm. However, the changing technological nature of the environment has brought new challenges to the applicability of these laws. Often, they have been forced to play catch up to confront cyberspace attacks, and even developing countries are still grappling with the challenge of enforcing self-defence laws without contravening other laws. This section demonstrates that the provision for the enforcement of self-defence laws poses unique challenges to the enforcement of the same laws in the cyber world. Therefore, although cyber attacks may bear the same characteristics of armed attacks, it is difficult for organisations to evoke self-defence laws, even those outlined by article 51 of the UN charter. Some of the unique challenges posed to the enforcement of self-defence laws in the cyber world include proportionality issues, the trans-national nature of cyber attacks, and the difficulty experienced in identifying the attacker. In spite of the legal debate, active defence is a reality، hence active SA needs to be understood in order to defend against it at the very least.

Besides the above challenges, it is similarly difficult to invoke self-defence laws (at least in the conventional way) in cyber attacks because cyber attacks (often) do not lead to direct loss of life, even though effects in the network have corresponding effects in real life. Therefore, there is a significant

mismatch between the uses of armed attacks (as a self-defence mechanism) in the physical world because it is difficult to satisfy the conditions for approving armed attacks in cyberspace.

The recent case in 2014 between Ukraine and Russia, when Russia took control of the Crimea, justifies the legitimacy of using active offensive action in cyberspace. The two countries were in a state of war, and Ukraine's (Kiev's) network infrastructure (communication network) was targeted, leading to massive disruption of the mobile network in Kiev (Lee, 2014). In this situation, Ukraine was already at war with Russia, and since Ukraine's cyberspace was targeted, then it should be legal for Ukraine to respond to the attack in order to defend itself. Consequently, active defence and active SA should be implemented so that nations can protect their interests from cyber attacks.

This section has highlighted the significant differences and similarities in the applicability of defence laws in the UK and the US. By the nature of their geography and distribution, both countries are subject to larger legislative provisions in their cyber laws. For example, the UK is a signatory to European laws on cyber attacks, while cyber defence laws that the federal government formulates also bind American states. Even though cyber defence laws continue to evolve in these countries, English common law is the basis of their enforcement. In America, the Bill of Rights also plays a critical role in the enforcement of these laws. Nonetheless, as the analysis in this chapter shows, there is a clear trend towards the militarisation of self-defence laws in cyberspace (especially in the US) (Greenwald, 2012: 2). Analysts should treat this trend with a lot of caution, because the militarisation of self-defence laws in the cyber world may fail to achieve the same objectives they would achieve in the 'real' world. It appears that cyber self-defence is a moot point, but the legitimacy of active SA and active offensive defence depends on the context and the level of threat a country's CNI faces, or whether it takes place in the context of an act of war. The question now presents itself: are active SA and active SA legitimised when implemented together with kinetic warfare activities (as in the Ukraine and Russia case)? It is therefore pertinent and important for international and local laws to encompass the unique dynamics of cyberspace attacks. The introduction of a new set of laws to accommodate these dynamics may be a good start for many countries to address the unique challenges of the cyber world so active defence and active SA can be developed correctly while lined and supported by law.

2.4 EMERGING POINTS AND ACTIVE SA HYPOTHESISED THEORETICAL FRAMEWORK

Within the context of this study, an important argument emerges from the literature review: If converting the SA into successful decision-making happens to be the central tenet of SA utilisation, and if it requires appropriate channels (knowledge/software programs) to obtain the desired outcome, then it should also be acknowledged that intangible channels such as Attitude or Outlook be considered as important instruments to achieve the desired SA utilisation (Endsley, 1995b, 2000; Tadda, 2008).
For example:

- Attitude 1: Defensive posture to deter cyber attacks (Defensive attitude)
- Attitude 2: Offensive posture to deter cyber attacks (Winning attitude)

The three SA models reviewed in this study clearly show their preference for Attitude 1, i.e. a defensive mindset which in turn influences the operator to process and utilise knowledge only within the concept of attack prevention. Accordingly, all of them focus most on analysing the nature of attacks in order to learn about the tactics employed by the attacker. Thus, in this case one can assume that the operators would gather certain knowledge only after the occurrence of an attack, instead of creating any knowledge that would be new to the attacker and would be capable of managing cyber operations without any hassle.

In contrast, Attitude 2 conforms to a military stratagem of Sun Tzu, where the operators would always be engaged in creating new knowledge, since Attitude 2 commands an attacking attitude to prevail over all possible cyber attacks. At this point, this researcher realises the gravity of adopting an appropriate attitude towards SA, since it highly influences the designing of systems; for example, Attitude 2, as mentioned above, could result in forming a mirror domain, could include operations such as invading the enemy's domain, could hoodwink attackers by sending them into a mirror domain, could collect information about what they want, and could misdirect them with false or fake information through deception techniques and so on.

Therefore, from the perspective of Attitude 2, all three models – the JDL Model (purely data-based model), Endsley's Model (mental model) and Tadda's Model (combination of JDL and Endsley's model) – appear to be suffering from uncertainty, while focusing mostly on self-awareness and confining their activities within the host domain. This assumption is consolidated when one learns that both Endsley (2000) and Tadda (2008) identify the shortcomings of their model in level 3 of SA, where new knowledge is required to nip the attack in the bud. Now, this study has argued that an attitude of only blocking attackers would never be enough to win the situation; instead, it would motivate the enemies to innovate, creating newer and innovative ways of attack.

Thus, one can identify Attitude 1 as a reactive approach (existing models) and Attitude 2 as a proactive approach (required new models), where existing models function as below:

Figure 2.9: Attitude 1: Reactive approach (existing models) (Source: Author)

2.4.1 Models Using the Reactive Approach Are Inadequate in the Present Context

Models using a reactive approach can be considered as low-resolution models in the present context. The increased dynamism of the cyber world is the first point that negates adopting a reactive approach, as it encompasses only past knowledge that can be used to address the enemy's attack. The futility of such an approach can be understood by anyone who keeps tabs on recent developments in the cyber world. For example, the Department of the US Army has observed that trends in the cyber world are changing rapidly, since Information and Communication Technology (ICT) is continuously improving in all areas of cyber operations. Accordingly, the army conducted an assessment that led to several indicators. First, the army's current vocabulary, including CNO (computer network operations), EW (electronic warfare) and IO (information operations) are increasingly becoming inadequate due to the emergence of several new cyber features. In order to address these challenges, the US army has introduced three interrelated dimensions, or full spectrum operations (FSO), where each dimension contains its own set of causal logic and commands a focused development of solutions. Therefore, active defence and active SA are already integrated into the US approach, as active SA is considered legitimate by the US army to use when deployed on a mission.

The first dimension of FSO refers to the psychological contest of wills against enemies who are implacable, warring factions, criminal groups, and other potential adversaries. The second dimension of FSO refers to strategic engagement, which involves keeping friends at home, gaining allies abroad and generating support or empathy for missions. The third dimension refers to cyber-electromagnetic contests, which involve gaining, maintaining and exploiting technological advantage (TRADOC, 2010). It becomes clear at this point that the cyber commanders require:

a) Winning the psychological contests of wills against enemies;
b) Creating quality local and global allies;
c) Winning cyber-electromagnetic contests.

Judging from the above perspective, one is forced to admit that the SA models that operate only with limited (past) knowledge, such as the Endsley/JDL/Fusion models, are low-resolution models, which do not have enough requisite variety to deliver what the cyber commanders require in order to achieve the above three goals, because all of these goals involve a diverse range of cyber operations, each commanding quality level 3 SA operations, requiring the application of new knowledge. We can recall at this point that both Endsley (2000) and Tadda (2008) identified the shortcomings of their respective models at level 3 of SA, where new knowledge, from a new source of intelligence, is required to nip an attack in the bud.

2.4.1.1 The risk quotient becomes very high

The gravity of SA becomes clearer when one reviews the relationships between the three pillars of any nation, being its cyber infrastructure, critical infrastructure and physical infrastructure. This can be depicted as below:

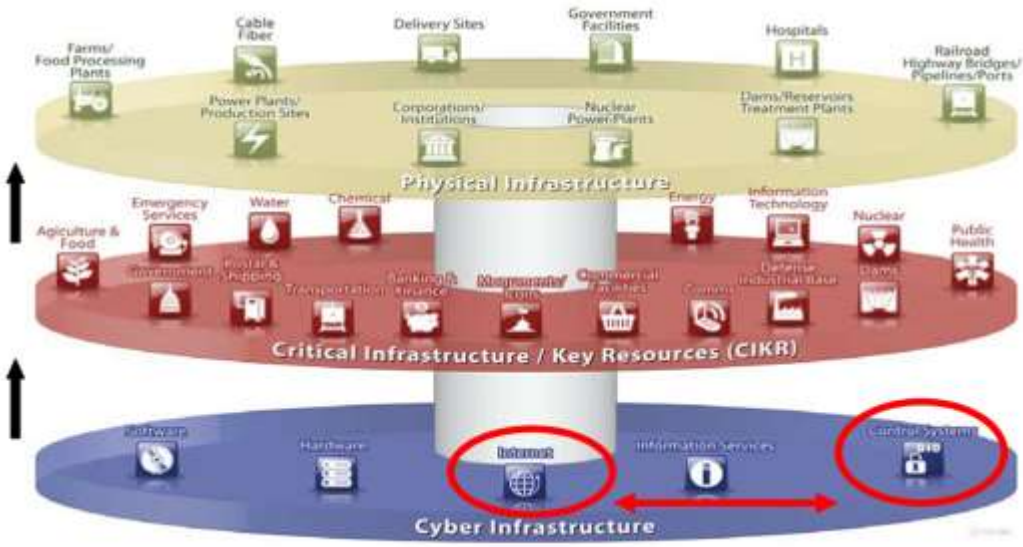


Figure 2.10: Physical, Critical and Cyber Infrastructural Relationships [adapted from DHS (2010)]

The above diagram clearly highlights several facts:

- First, at the national level, the critical and physical infrastructures are fully dependent on favourable interactions between the Internet and the control systems.
- Second, at the local level, each component of the critical and physical infrastructures requires appropriate cyber security to carry out its function.
- Third, the wired and wireless connections between the components of the critical and physical infrastructures require appropriate cyber security to carry out transactions.

Such preconditions clearly establish the fact that the issue of cyber security is extremely important at national, local and inter-infrastructural levels. Therefore, one has to concede that the idea of waiting to

gain knowledge from an instance of attack in order to use it in a post-attack situation could prove fatal for a nation as a whole, especially when the issue is viewed from the perspective of the security of the critical and physical infrastructures. Therefore, this strongly prompts the inference that adopting Attitude 1, i.e. the reactive approach, could by very risky, as it allows the enemy to apply its new knowledge in attack, while the defender has no clue regarding the possible magnitude of the possible damage involved. Therefore, the models based on the reactive approach, such as Endsley's, JDL's and the Fusion models clearly appear to be risky investments, as their failure could be disastrous for a nation. Therefore, a new model to overcome this risk inherent to the reactive approach is required.

2.4.2 Benefits of the Active Approach in the Present Context

On the other hand, the required new model's active approach, influenced by Sun Tzu's military strategy, is set out in Figure 2.11.

Figure 2.11: Attitude 2: Proactive Approach According to Sun Tzu's Strategy (required new model) (Source: Author)

The above differences between the existing models and the required new model can also be termed Passive SA and Active SA. A classic passive CND (cyber network defence) is composed of multiple niche intrusion detection tools, such as password protection, data encryption and firewalls, which carry out network data analysis and produce unique alerting outputs (Beaver et al., 2011). Therefore, a CND is totally reactive in nature, as it acts only after the attacker has inflicted a certain degree of harm on the network. Passive defence typically reacts to pre-defined techniques, such as disabling an account after three incorrect logins and notifying the administrator by email of the event; but this could be ignored and result in the need to start an investigation into why the account was deactivated, and what was the cause (whether the user forgot her/his password or whether it was a hacking attempt). Altogether, these tools are inadequate in the sense that hackers devise techniques to penetrate them and launch attacks (Holdaway, 2001). In the preceding sections, we have seen that the standard understanding and application of SA theory in cyberspace has severe limitations, namely its reliance on intelligence captured from local networks; it does not capture all the possible attacks in the environment, nor is it dynamic enough to tackle the innovative techniques of cyber attackers, and it activates only when incidents occur, and when it is too late to defend.

In contrast to the cyber security approach, active defence comprises measures originated by the defender against the attacker, which not only thwart the attack in progress, but also ideally make it difficult to launch more attacks. Active SA and active defence are about taking the initiative to deny the cyber attackers from achieving their purpose. Holdaway (2001) categorises them into three types, namely:

1. Counterattack – can be conducted against the attacker's information system during or immediately after the initial attack.
2. Pre-emptive attack – aimed at the enemy's information system infrastructure, it is designed in such a way that it will deter the enemy from launching effective attacks against the network systems.
3. Active deception – uses the momentum of the attack to defeat it by channelling an attack away from the defender's information scheme and into a practical mould of it. This makes the attacker believe it is successful, when in actuality it is neutralised.

For example, active SA might use Benware to act as a law-enforcement Trojan to infiltrate the attacker with the agent that can help in gathering information about the attacker and discover what they are planning. Such intrusions can include live video feeds, screenshots and/or basic data streams (Varon, 2002). This will allow the defenders to be active in the enemy's domain so that more reliable intelligence will be fed into their cyber SA, which will eventually lead to better cyber security.

In addition, Benware can be used over time to investigate the information on the attackers' system and use it to gather information about them. The possibilities are truly endless in this case, and the location of the attackers could be tracked easily, since Benware could help eliminate the capabilities of the proxies used to cover the attackers' the paths. Benware can establish direct connections to the operator in order to triangulate the location of the attackers. It can also act as a client through which to issue various commands that can be performed on the attackers' devices/computers upon request (Theohary & Collins, 2011).

Upon gathering enough information, the operator could use Benware to act as a law enforcement Trojan, whereby the operator would infiltrate the attackers' system with the agent, which can help in gathering information about the attackers and know what they are planning to do next. This could include a live video feed, screenshots and/or basic data streams (Chen, 2010).

2.4.2.1 Anticipated advantages of active defence

Essentially, the best defence is a strong offense, and many countries have adopted this offensive strategy to deny criminal or terrorist forces' attempts to control or use the Internet for their own illegal purposes through the creation of good botnets (Theohary & Collins, 2011). Furthermore, active defence involves constant patrolling in cyberspace, and such patrols can detect, deny, pursue and destroy websites, malicious software and several other cyber agents and computer hardware held by those with

criminal and/or terrorist intentions (Varon, 2002). In addition, patrolling offers faster and more accurate information about future threats, including their source, machinery and architecture. This enables an organisation to upgrade its intelligence system to a level from where it can scan many nodes and secure vital intelligence. This in turn makes the organisation far more capable of detecting the type of attack, the movement of the attacker within the network, any security credentials that have been compromised and what data have been stolen or destroyed (HBGary, 2013). Finally, it works as a real threat of counterattack/response, making the hackers wary of conducting an attack in the first place, in addition to delivering tangible means of penalising them.

2.5 Hypothesised Theoretical Framework and Active SA Model

The essence of the review generates the following points underpinning this study:

1. The cyber commander should possess an attitude/mindset of being offensive in taking on all cyber attacks, instead of adopting a defensive attitude;
2. Such an attitude would encourage the operator to decisively create new knowledge, as a winning attitude within this context requires new knowledge;
3. The cyber commander then should create and exploit new knowledge through appropriate channels, such as an appropriate SA model, which would enable the operator to exploit multi-domain ambience, invade attackers' domains, and apply deception tactics;
4. An aggressive strategy appears capable of defeating the attackers even before they can resort to any harmful operation in operator's domain;
5. Finally, the operator should be able to achieve the desired outcome, i.e., managing, retaining and improving the desired cyber operations.

Such preconditions can be framed in the following manner:

Figure 2.12: Theoretical Framework Emerged from Literature Review (Source: Author)

No one can deny the fact that most of the organisations dealing with sensitive data relating to one or more infrastructures of national importance cannot afford to wait for an attack incident to occur and then react, because the consequences may already be severe at that point. Such a state of affairs thus consolidates the argument in favour of a more proactive and offensive approach to effectively protect the network. Therefore, the findings of the literature review demands formulation of a new channel, i.e. a new SA model or system that would complement the winning attitude, such as enabling the cyber

commander to employ an appropriate deception technique involving a multi-domain environment. It is here that the Active SA Model (ASAM) proposed by this study fits in, where its tasks within the context can be framed as below:

- ASAM will interact with adversaries;
- ASAM will be activated once an attack gets redirected;
- ASAM will use deception (new knowledge for the attacker) through redirecting the attacker to a deception server;
- ASAM will use spyware such as Benware, if so needed, to control the adversaries and to get into their domain;
- ASAM will influence the enemy through deception, which will affect their own SA.

The cutting edge aspect of ASAM would be the new knowledge it generates, which would act as the force multiplier. The tasks mentioned above highlight the role of intelligence (creation and application of new knowledge), which in turn helps this study to further narrow down the role of ASAM to create a compact theoretical model, in the following manner:

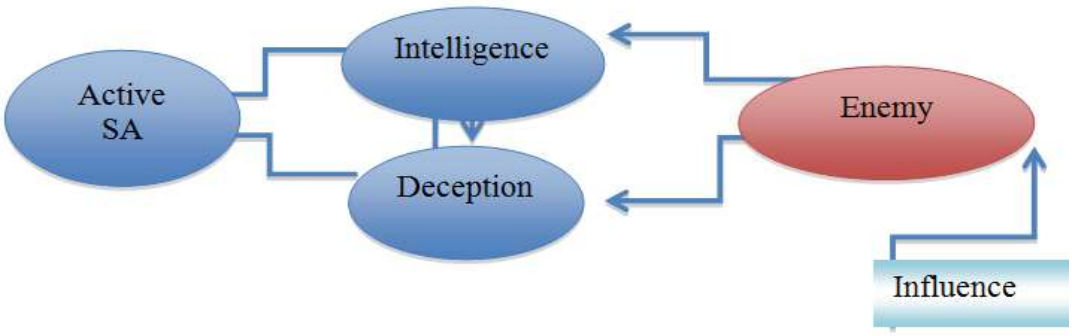


Figure 2.13: Compact Hypothesised Theoretical Model of ASAM (Source: Author)

We have argued the role of intelligence is extremely crucial for an endeavour such as the creation of the ASAM model, which needs to be continually updated with knowledge regarding the possible enemies (capabilities, resources, plans, motives etc.), since that knowledge will form the basis of a counter action. However, there is no literature on any specific type of cyber intelligence that can be exploited within this novel context except the concept put forward by Sun Tzu, who specifically focused on the intelligence of one party used to defeat the other. His strategy involves the concept of yin and yang in Taoist philosophy, which suits the cyber situation well, since it covers all possible situations, especially where the issue of intelligence is involved. For example, the integration of networks takes place in the mind of the commander, which includes cyber support and the intelligence fusion centre. By deception in cyberspace, the mind of the commander can be attacked (Cahanin, 2011; Nakashima, 2010; Thomas, 2009). Thus, the merit of the above concept prompted this researcher to rely on the variables situated in the framework of this model (Table 2.7). This study has also taken a leaf from computer forensics, which is a process of constructing cyber incidents and understanding

incident kill chains, besides aiming to define and identify hackers, hacking impacts, the resources and tools involved in hacking, and enemy plans and their motives. Altogether, the literature prompted this study to believe that commanders in a cyber war should direct their intelligence operations to focus on gathering information that allows denying the cyber attackers from achieving their purpose.

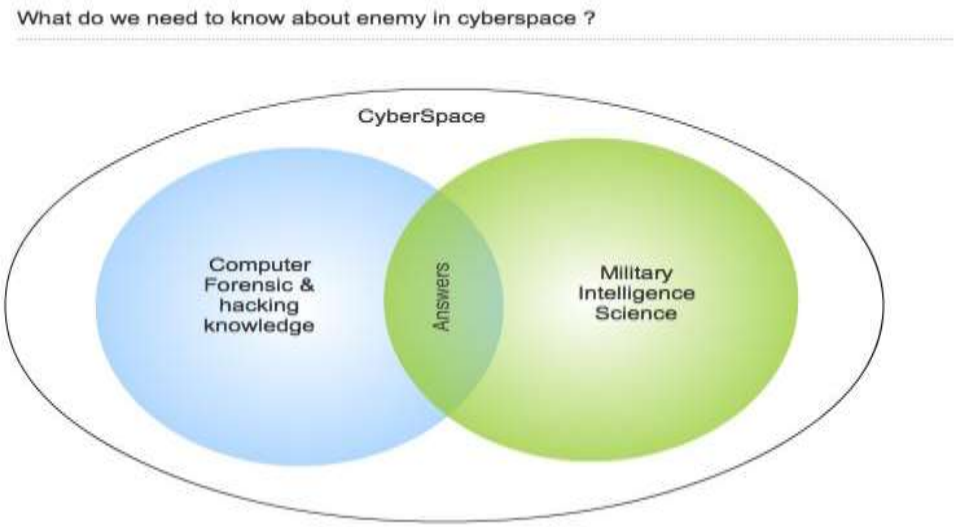


Figure 2.14: Knowledge and Intelligence Involved in SA (Source: Author)

Since a cyberwar is no less important than a real-time war as cyber is an integral part, it is part of the global commons, it becomes pertinent to consider the eight interrelated variables recommended by the United States Army's (2010) Cyberspace Operations Concept Capability Plan 2016-2028. Those variables are political, military, economic, social, information, infrastructure, the physical environment, and time. The said recommendations appear highly important for any cyber SA model for answering the following questions, which together can be termed the Safety Framework:

1. Who is the enemy?
2. What is the enemy's motive behind the attack?
3. What is the location of the enemy?
4. What is the goal of the enemy?
5. What is the capability of the enemy?
6. What is the weakness of the enemy?
7. What could be the impact of attack on the operator's domain?
8. How could the attack be defused beforehand?

However, considering the gravity of the threat to cyber security, as reviewed earlier, the proposed ASAM requires integrating military philosophy in its structure and mechanism. Accordingly, it should utilise 13 military recommendations from Sun Tzu's *Art of War* (AoW) under four categories: *Initiation*, *Direction*, *Action*, and *Exploitation which shape the process of active defence.*

Category 1: Initiation (What is the situation?)

Under this category, ASAM would allow commanders to first deal with basic knowledge (identifying the possible enemies), and then would formulate the basic line of action by utilising Sun Tzu's AoW I (Laying Plans) and AoW IV (Tactical Dispositions). According to AoW I, good leaders not only exploit flawed plans, but also exploit flawed adversaries (Parks & Duggan, 2001; Sawyer 1994). Furthermore, the interpretation of AoW IV from the perspective of a cyber war suggests that the primary challenge in cyber warfare is to know whether the system is under attack, and therefore the short-term cyber defence goal should be to improve an organisation's ability to collect, evaluate and transmit digital evidence (Geers, 2011). Both of AoW's sub-categories thus point to the importance of gathering appropriate inputs about the enemy, and therefore the commander would have to deal with four variables in this category, which are Enemy Identity, Enemy Location, Enemy Motive and Enemy Goal. These provide the basic information which the commander cannot do without.

Accordingly, the activities that fall under this category would involve the use of passive intelligence, where security alerts would send tacit knowledge that could be converted into explicit knowledge by virtue of intelligence gathering when the commanders start identifying important variables about the enemy.

Category 2: Direction (Where Am I Going?)

Under this category, ASAM would develop the above plan in detail, besides understanding the possible magnitude of the power of the enemy. At this stage, ASAM would utilise AoW IX (Army on the March) and AoW X (Terrain). According to AoW IX, much like in real-time war, cyber commanders too need to check all nuances of the system while counter attacking the enemy, and should always remember that attackers too can apply deception (Sawyer, 1994). Alongside this, AoW X suggests that cyberspace contains more dangers than the real world, since terrestrial distance does not play any role while one is connected to the network. Cyber weapons are also unreliable in character, since they are prone to reverse engineering. Thus it takes meticulous pre-operational cyber attack planning and timely application to manage the cyber terrain (Parks & Duggan, 2001). Both AoWs thus point at the importance of gauging the enemy from all sides, which in turn would lead the commander to deal with three variables in this category, which are Enemy Capability, Enemy Weakness and Possible Impact of Enemy Attack.

Accordingly, the activities within this category would involve usage of the Explicit Knowledge acquired from the activities of Category 1, which would enable the commander to gauge the enemy from all sides and to decide on the course of action.

Category 3: Action (How Am I Going to Do That?)

Within this category, ASAM would allow commanders to launch an attack on a cyber explorer who has already been tracked down as a lurking prowler. At this stage ASAM would allow commanders to utilise AoW II (Waging War), AoW III (Attack by Stratagem), AoW V (Energy), AoW VI (Weak and Strong Points), AoW VII (Maneuvering), AoW VIII (Variation in Tactics) and AoW XI (Nine Situations). Since this category uses the most number of Sun Tzu's military advice, it is pertinent to describe them in brief:

AoW II: The cyber commander would collect the credentials and privileges of the enemy without letting the enemy know about it (Addinall, 2012; Geers, 2011). This would be done to ensure the safety of the commander domain. This is tantamount to ethical hacking, since the commander does this only after being convinced about the enemy's evil intentions.

AoW III: If the cyber war involves the IT infrastructure, a cyber-only victory is the only way to protect the same. Therefore, it is important for the commander to secure victory before combat is even necessary (Sawyer, 1994).

AoW V: This is a win-or-perish situation, and therefore it is expected that the enemy will apply all its power and skill to outrun the commander, and therefore the commander must remain one step ahead by consistently applying all of the skills of war, and hit the opponent at the most opportune moment (Geers, 2011).

AoW VI: The commander would make all adversaries' cyber reconnaissance difficult and confusing to the enemy, so that the enemy falls short of developing an effective strategy (Sawyer, 1994).

AoW VII: Much like in a real-time war, the commander would deceive the enemy through misinformation before going for the final kill (Parks & Duggan, 2001).

AoW VIII: The commander would treat every combat situation as a new situation and approach it with all alacrity, and would not sit complacent on happy memories of earlier success (Sawyer, 1994).

AoW XI: Much like in a real-time war, the commander would keep checking on all the nuances of the system while counter-attacking the enemy, and would also keep in mind that the enemy too can apply deception (Sawyer, 1994).

The above suggestions would lead the commander to deal with three variables in this category, which are Timing of Attack, Consistency of Action and Variation in Action. Accordingly, the activities within this category would contribute to the commander's intelligence, which in turn would expand the possibilities for exploiting the enemy.

Category 4: Exploitation

Under this category, ASAM would work on exploiting the frustrated state of the enemy, such as deceiving and cornering the enemy in order to extract more knowledge about the enemy, its motive and goal. Here, ASAM would utilise AoW XII (Attack by Fire) and AoW XIII (Use of Spies). AoW XII suggests that the commander should annihilate the enemy, while AoW XII suggests using spies to get more information in such a situation. Such suggestions would lead the commander to deal with two variables in this category: Knowledge Collection and Demolition.

Knowledge Collection and Demolition can work in tandem and enable the commander to launch offensive and deception processes. This active state of cyber SA, coupled with the passive state of cyber SA, will generate a comprehensive intelligence, which would then contribute to the dynamics of Perception, Comprehension and Projection, which in turn would contribute to SA Agility and SA Quality.

It is worth noting that cyber commanders should always engage in categories 1 and 2, as the situation is dynamic and ever-changing, so cyber commanders need to be alert to when the situation in the environment changes. Also, re-planning and setting a new direction is required in cyberspace because there is no plan that survives contact (Clausewitz, 1976). However, with an active defence strategy, re-planning is possible to achieve due to the fact that intelligence from the enemy's domain will be captured, allowing cyber commanders to set a plan before the enemy takes action.

2.5.1 Enhanced Hypothesised Theoretical Model of ASAM

The cyber domain and cyber attacks are always evolving, and cyber incidents happen in a fraction of second; an agile response should then be in place to deter and defend networks. This literature review has identified and explained the variables of the new, enhanced SA model (Table 2.7), where intelligence factors directly impact SA. The enhanced SA in this model is achieved through utilising the offensive capability that allows defenders to interact with suspect attackers in order to gain new knowledge, meaning that active intelligence becomes critical component part of the enhanced SA model. Active intelligence in the new, enhanced model is introduced because it has been argued that being passive in cyber security is inadequate. Passive intelligence and intelligence gathering capability along with SA represents the current state-of-the-art of SA models. One current model, such as Tadda's (2008), is passive, since it monitors only local networks. Also, all other, previous models have no factors that allow us to assess how good a particular SA is. Therefore, this research believes in the importance of having a measurement factor that determines how good is the personnel SA by measuring the quality of their SA and their agility in achieving it.

Finally, the cumulative power of active intelligence in ASAM, it is argued, would greatly enhance SA, which in turn would help the commander to frustrate the enemy to the fullest. The proponent of this model recognises the fact that the level of the qualities of the three major components of this model,

i.e. perception, comprehension and projection, would depend on the qualities of several factors. For example, the quality level of perception would depend on the quality level of intelligence, while the quality of intelligence would depend on the qualities of correctness and completeness. In the same fashion, the quality level of comprehension would depend on the quality levels of previous knowledge, skills and experience, analytical ability and confidence. Finally, the quality of projection would depend on the intent, i.e. the desired outcome. Therefore, Enhanced SA can be measured using the quality and agility variables (Table 2.7) to determine how good the SA performance is, which is critical to SA evaluation.

Therefore, covering issues ranging from Basic Knowledge to Advanced Knowledge, the enhanced theoretical model of ASAM would look like (Figure 2.15):

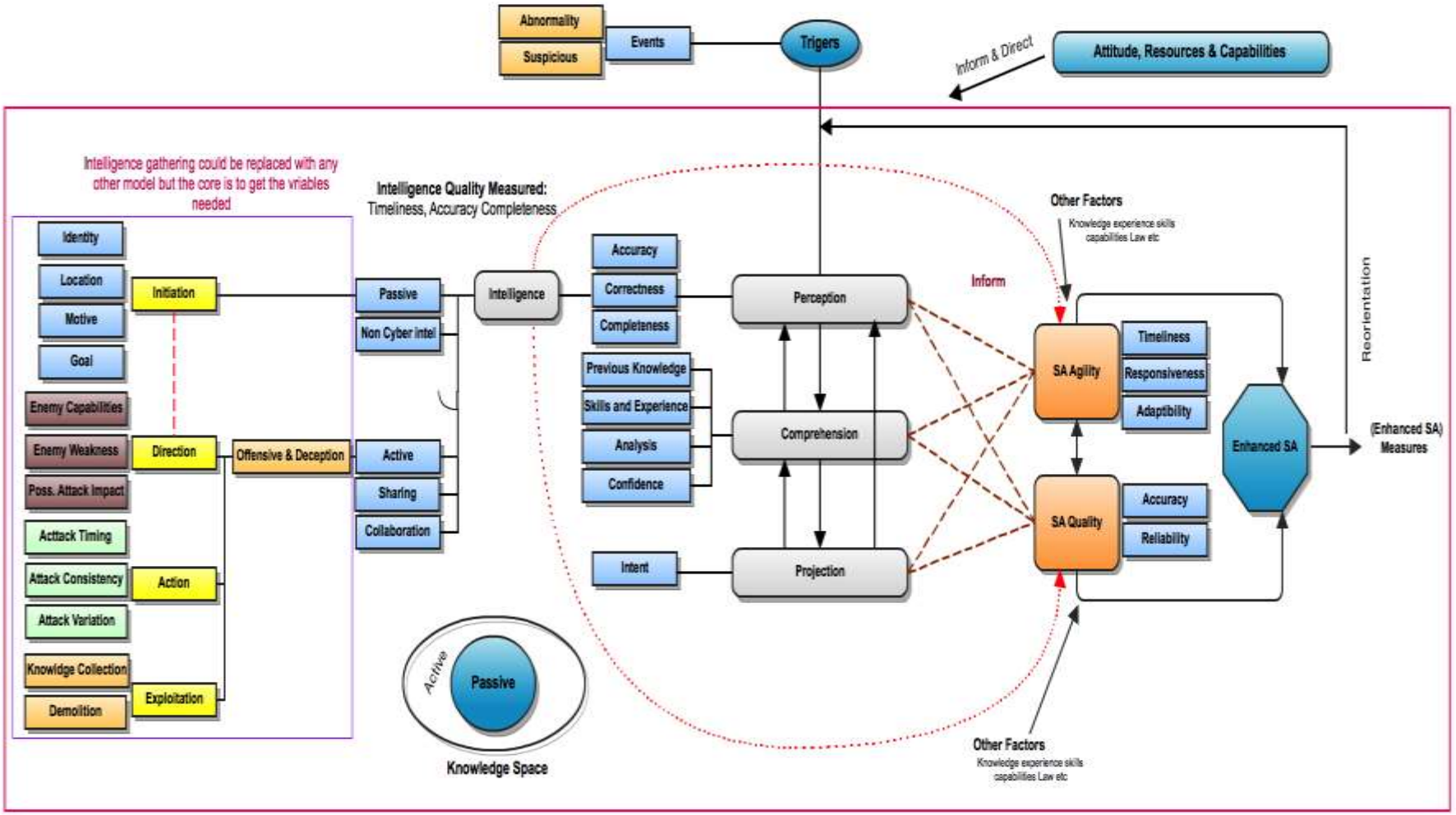


Figure 2.15: Enhanced Hypothesised Theoretical Model (ASAM) (Source: Author)

One might question at this point how ASAM could perform so many tasks. This can be answered by stating that the main driving force of ASAM is intelligence generated from new knowledge (gathered from the adversary domain), which would operate with enhanced ability to deter cyber attacks since it is consistent with military doctrine. Figure 2.16 represents the mechanism of ASAM.

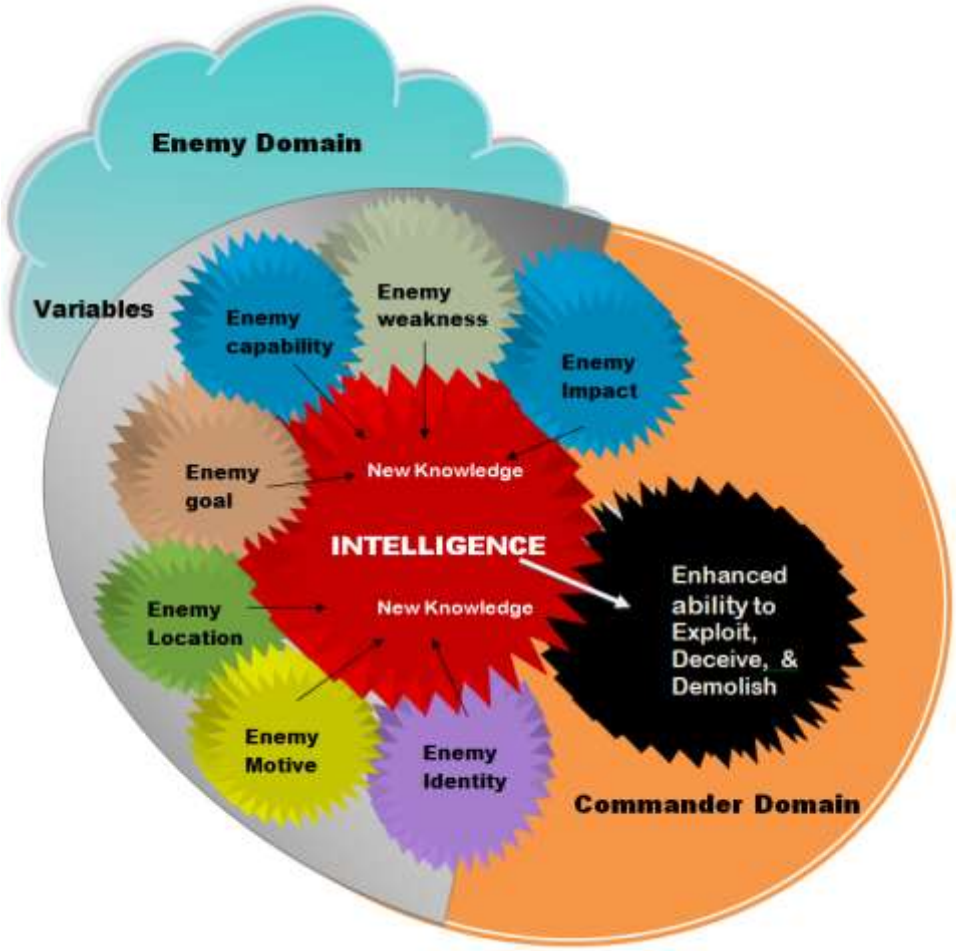


Figure 2.16: Mechanism of ASAM (Source: Author)

The above diagram makes it clear that, in ASAM's case, a continuous flow of intelligence would give the upper hand to the operator dealing with security threats even before their occurrence. For example, ASAM would influence (Figure 2.9) the attacker by exploiting the OODA loop (Observe, Orient, Decide and Act), which is a decision-making model and part of Colonel John Boyd's Asymmetric Fast Transient theory of conflict (Boyd, 1987). The central tenet of OODA theory from a military perspective is to defeat the adversary strategically, by psychological paralysis (Value Based Management, 2011). Here, the basic difference between ASAM and the reviewed models becomes prominent once again, since ASAM works by gathering new knowledge from the adversary domain and feeding that new knowledge into the organisation's SA – specifically into the comprehension phase, which in turn can diffuse any attack even before it occurs.

ASAM comprises several factors (Table 2.7 and Figure 2.15). SA on its own is a combination of perception, comprehension and projection. In previous literatures (Tadda, 2008; Endsley, 1995; see section 2.2.3), researchers discussed how information feeds into perception; however, they were not

clear enough about what to perceive. Tadda's model provides some basic information about data-gathering and the importance of intelligence feeding at level 0 of his model, but in his research Tadda does not explicitly cover what information is to be gathered; also, the model focuses only on the passive intelligence gathered from the defender network (Tadda, 2008). For that reason, SA and passive intelligence factors together represent the current passive SA model that relays only the information that comes from the local domain. On the other hand, the core of the proposed ASAM in this research is the active intelligence factor that facilitates interaction with adversaries, with the aim of gathering intelligence from their domain as well as accruing passive intelligence. In ASAM, this type of intelligence comes from previous knowledge or experience regarding cyber incidents, risk assessments of cyber resources, politics or deception, as discussed earlier, whereby adversaries can be channelled into manageable or controlled cyber resources for the purpose of gathering intelligence. Finally, ASAM integrates the principal factors that allow measurement of the performance of cyber commanders' SA, since cyber incidents require an agile SA that exploits quality active intelligence when dealing with cyber attacks.

2.5.2 Comparison between Active SA model and current SA models

At this juncture of the critical review it becomes pertinent to compare the three SA models reviewed in this study, as well as the promises offered by ASAM under the context of the safety framework set out below, which advises defeating the adversary well before it can do any harm to the network. Table 2.6 shows the comparison between 3 main SA models with active SA. The variables in the table were extracted from the literature discussed earlier. Also, the table lined the variables with active SA so better understanding can be developed in the area of active defence.

Table 2.6: Analysis of SA Models within the Safety Framework

[Synthesis of all Review Points]

Situation Independent Variables		JDL	Endsley	Fusion	ASAM
Winning Attitude		No	No	No	Yes
Defensive Attitude		Yes	Yes	Yes	Yes
SA Agility	Timeliness	Yes	Yes	No	Yes
	Responsiveness	No	No	No	Yes
	Adaptability	No	No	No	Yes
SA Quality	Accuracy	No	No	No	Yes
	Reliability	No	No	No	Yes
Situation Dependent Variables		JDL	Endsley	Fusion	ASAM
INITIATION	Enemy Identity	No	No	No	Yes
	Enemy Location	No	No	No	Yes
	Enemy Motive	No	No	No	Yes
	Enemy Goal	No	No	No	Yes
DIRECTION	Enemy Capabilities	No	No	No	Yes
	Enemy Weaknesses	No	No	No	Yes
	Possible Enemy Attack Impact	No	No	No	Yes
ACTION	Timing of Attack	No	No	No	Yes
	Consistency of Action	No	No	No	Yes
	Variation in Action	No	No	No	Yes
EXPLOITATION	Knowledge Collection	No	No	No	Yes
	Demolition	No	No	No	Yes

Table 2.6 shows that the JDL/Endsley/Fusion models fail to address the above-mentioned situation-dependent variables, which in turn exposes their severe limitations in providing quality cyber security that could demolish the enemy before it can do any harm to the network. On the other hand, ASAM proposes to address all of the above situation-dependent variables, which makes it an ideal SA model in the present context.

Table 2.7 summarised the variables extracted from this thesis literature for the conceptualised active SA model which will be used for designing this research survey. Therefore, the data collected from this survey will be analysed using Structural equation modelling to extract the causality model of Active SA.

Table 2.7: Variables of Enhanced Situational Awareness (see Chapter 3 and Appendix 1 for more detail)

Perception	Correctness: The extent to which awareness is consistent with ground truth (Albert & Hayes, 2006: 124).
	Completeness: The percentage of relevant information attained (Albert & Hayes, 2006: 125).
Comprehension	Previous Knowledge: The explicit knowledge which serves to formulate decisions and to generate new knowledge by fusing it with tacit knowledge (Nonaka & Nishiguchi, 2001).
	Skills and Experience: Ability to acquire new knowledge and the ability to convert both new and explicit knowledge into desired action (Nonaka & Nishiguchi, 2001).
	Analysis: Systematic unravelling of knowledge and understanding.
	Confidence: Willingness to use the information ((Albert & Hayes, 2006: 125).
Projection	Intent: The will to perform an act (Salerno & Tadda, 2009: 1).

SA Agility	Timelessness: A state of eternal existence, such whether ASAM is capable of constantly producing new knowledge and enhancing the ability to diffuse the attack before its occurrence (Albert & Hayes, 2006: 125).
	Responsiveness: The ability to act within windows of opportunity (Albert & Hayes, 2006: 125).
	Adaptability: The ability to adapt to changes quickly, or the ability to alter processes and organisation to improve effectiveness or efficiency (Albert & Hayes, 2006: 189).
SA Quality	Accuracy: The quality of nearness to the truth, or the true value or the quality and usefulness of knowledge provided (Endsley & Robertson, 1996; Albert & Hayes, 2006).
	Reliability: The quality of the sources used to produce SA (Albert & Hayes, 2006).

Intelligence Gathering	Passive data collection: is the process of collecting network data of people interaction across the network or process to capture network traffics in an organization that data are being collected from them using local security sensors (Huey & Rosenberg, 2004: 598; Beaver et al., 2011).	IP identification: Identifying the location of a network service user by use of IP address (Gordon, 2005).
		Geo-Location: Identifying the actual geographical location of a user through the computer terminal connected to the Internet.
		Motive: The reason behind performing a given act (Varon, 2002; GAO, 2000)
	Active data collection: Intelligence collection is not disguised. This can be through installation of physical data collection devices, as described by Chen, Tan, Xing, Wang & Fu (2010: 1739), or through utilisation of hacking methods (Varon, 2002), through collaboration with Internet service providers (ISPs) (Huey & Rosenberg, 2004: 600).	Capabilities: Ascertaining the origin of a given cyber attack. Tracking cyber traffic and Enemy strength and resources (Holdaway, 2001)
		Weaknesses: Enemy weak points that can be exploited.
		Attack timing: Initiation of the attack at a time when it is most appropriate (GAO, 2000).
		Attack consistency: Extent to which attacks are similar and sustained (GAO, 2000) and the strength of enemy attack.
		Knowledge collection: Gathering of information, which could be active or

		passive (Chen, 2010).
		Demolition: Destruction of the enemy plans.

Intelligence	Timelessness: Right timing in order to prevent attacks from occurring. Helps organisations to predict the next possible attack, the mode of attack or the areas vulnerable to attack (Peterson, 2013).
	Accuracy: Precise information as to who propagates the attacks, when or where they are initiated (Lehr & Pupillo, 2009).
	Completeness: Comprehensiveness of intelligence. Pockets of information can be pooled through private and public sector collaborations to make meaningful conclusions (Amin et al., 2003).

2.5.3 Active SA Process model

In order to effectively enhance situational awareness, ASAM has to be implemented via a given process. This is carried out in three major steps. First of all, there is the passive perception or alert stage. The alert stage is noted through passive action (Palermo & Kocsis, 2005). Immediately, the active mode is initiated. This aims at identifying who the hacker is, why the attack is being instituted, the location from which the attack is orchestrated and other relevant information on the hacker. This can include the attacker's identity, motive, location, goal, capability, weakness and impact. This information is gained through the offensive method.

The second step is high level interaction, where the enemy domain is actively accessed. At this point, the offensive mode is in full swing. The enemy's domain is hacked, reckoned and scanned. Some of the issues that are discovered include the operating system that the attacker is using, the ports that have been opened and the services that are being run. This helps to know the domains that are vulnerable. This step also helps to give all the necessary information for countering the attack (Gordon, 2005; Wang, 2006: 178).

The last step of the process is the resource database mobilisation. At this point, the active domain is prepared to counter the attack. The identified vulnerabilities are sealed so as to make sure that the hacker has no access to the system. Furthermore, the cyber commander or computer network operators in the active domain already have an idea of what is in the hacker's mind. As such, it is possible to take the necessary protective measures which would ensure that the domain remains safe and impenetrable to the attackers

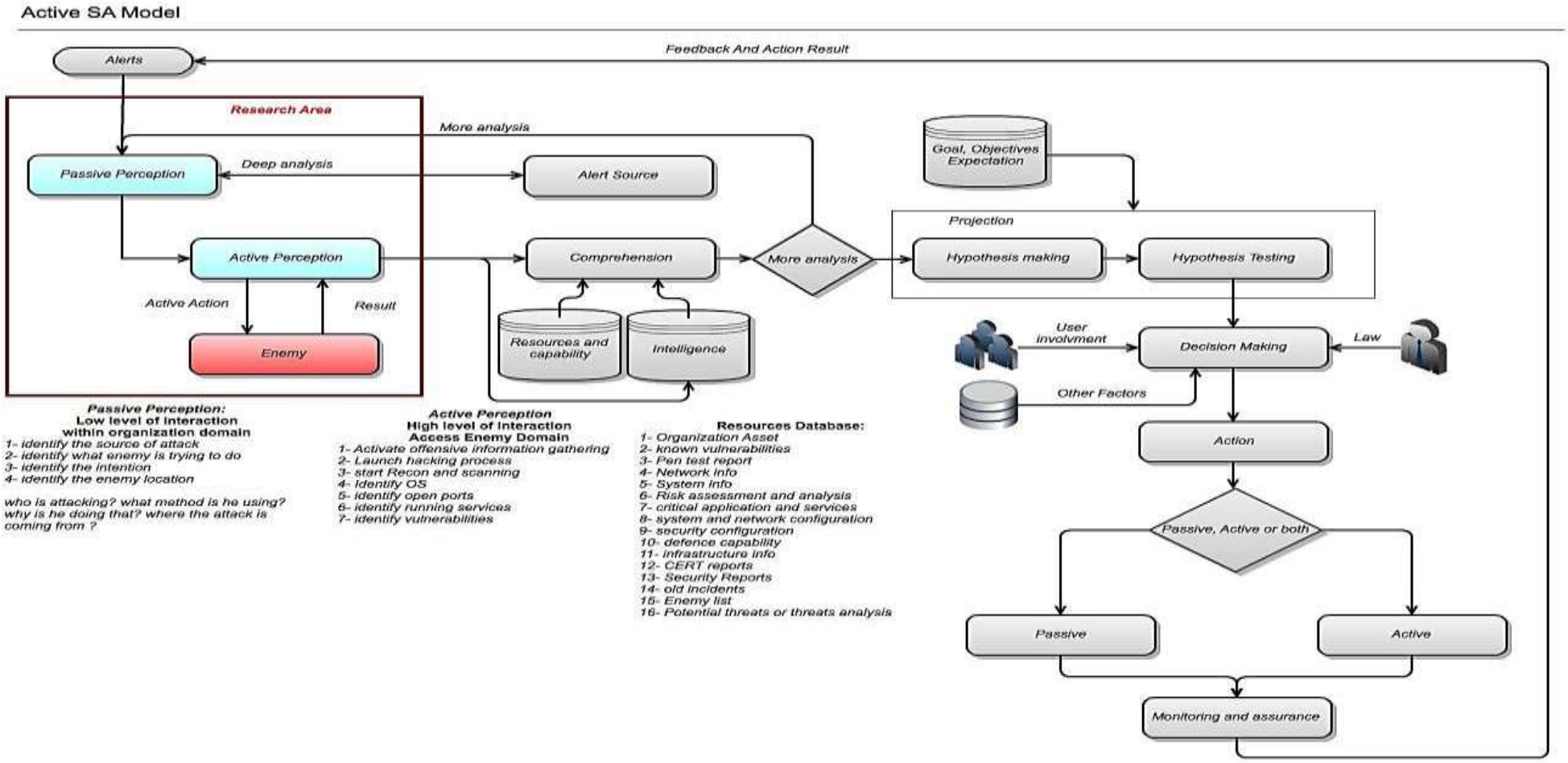


Figure 2.17: ASAM Hypothesised Process Model: (Source: Author)

Altogether, the theoretical findings identify the set of actions proposed by ASAM as the best set of actions for cyber security. However, ASAM requires undergoing the rigors of evaluation through real-time laboratory testing on a cyber range to prove its efficacy and effectiveness. Therefore, The ASAM theoretical model after being validated through SEM has informed the design of the process model which will be used in the experimental design to develop the data collection plan. Moreover, the variables identified in Tables 2.6 and 2.7 have been used to develop a framework for assessing SA and the utility of the proposed ASAM in practice using the cyber range in a Serious Gaming Experiment. This approach to SA evaluation not only serves to evaluate whether ASAM enhances SA but also provides the means to directly measure SA performance (combining Measure of SA Effectiveness, MoSA Efficacy and MoSA Efficiency) in order to determine SA Training, Techniques and Procedures for a Cyber Commander. Chapter 3 of this thesis will discuss these points in detail.

2.6 CONCLUSION

This research activity focuses on coming up with a new approach towards ensuring cyber security. The motivation behind coming up with the new model lay in the fact that the current models (JDL, Endsley and Fusion) lack in terms of agility and quality. They are also reactive (passive) in nature, implying that they cannot help in enhancing cyber SA in a world where there are new developments coming up day after day.

ASAM is designed in such a manner that it is proactive. It employs offensive mechanisms to break into the enemy's domain, actively collect intelligence form the domain, and also secure information on the enemy's variables such as the intent, potential, threat, location, capability and possible impact of the attacker's actions. All these variables give vital information that go a long way in ensuring cyber security. ASAM also helps in reducing the vulnerabilities in the governmental and other private sector organisations, as they can pool all the information they need to protect themselves from the attackers. In this chapter the design of ASAM is set out, and a cyber environment is proposed for testing of the same.

Based on the literature review, it can be argued that ASAM is hypothesised as being superior to the other SA models due to its active, offensive nature. Unlike the other models, ASAM helps in gathering intelligence in a very timely manner. It is also highly accurate, since the information is offensively attained by hacking the enemy's domain. As such, the intelligence gathered has all the desired characteristics of cyber intelligence. It meets the criteria for accuracy, completeness, timeliness and reliability. As such, the decisions made with regard to the data are well informed, and the protective measures derived from this information are made precisely by being customised to counter specific enemy attacks. Therefore, ASAM confirms the argument that active defence with an offensive approach is quite important in gathering intelligence from enemy networks, enhancing the agility and quality of cyber situational awareness and, consequently, helping deter cyber attacks.

CHAPTER 3: RESEARCH METHODOLOGY

3.0 OBJECTIVES & OVERVIEW

The purpose of this chapter is to provide a critical review of the candidate research methodologies. The approach promulgated in this thesis uses a combination of methods in order to achieve the research aim and objectives: to investigate whether an active offensive hacking method is more capable of enhancing cyber SA agility and quality than the existing SA models. This aim stems from an ultimate aim of contributing to the understanding of the concept of cyber situational awareness. Accordingly, the study contains five objectives:

1. To determine and critically analyse the current SA models and identify the key dimensions and variables for active cyber SA;
2. To develop a theoretical framework for active SA;
3. To evaluate active SA deployment in a serious gaming environment;
4. To develop a method framework for assessing cyber SA; and
5. To empirically assess the significance of effect and the implications of active defence in enhancing cyber SA agility and quality.

This chapter discusses in detail the methods employed, and provides a justification for their use. Data collection instruments and data analysis methods are considered. Scenario development and serious gaming environments are also discussed within the experimental design.

3.1 METHODOLOGICAL REVIEW

The sole aim of this study is to provide a comprehensive, high-speed and cost-effective active cyber SA model. Accordingly, the researcher probed the nuances of various research methodologies before opting for a mixed method whose efficiency has been proven in social science (Creswell, 2003), i.e. through a combination of both qualitative and quantitative research methods. This approach was adopted for several reasons.

First, the qualitative method banks on the collective wisdom gathered from the extant literature and the wisdom of a given researcher in the field, as developed through the processes of the research journey, from a specific situation to a general situation, where concepts emanating from events and human perceptions enrich the researcher's understanding (Bryman & Bell, 2003; DeVault, 2012; Guidestar, 2003). Such processes promised to be important drivers of this research, because the area of research was relatively new and the present researcher had great need to learn from the pioneering works of those who had come before.

Second, the quantitative method employs a deductive approach that considers the potential causes of something, and accordingly tries to verify the effect of the same through objective, quantitative and statistically valid measurements (Bryman & Bell, 2003; DeVault, 2012; Guidestar, 2003). Within the

context of this study, this method also promised to be an important research driver, as it promised to provide tangible evidences for arriving at a conclusion regarding whether the proposed Active SA Model (ASAM) could provide the desired cyber SA solution; i.e., to ascertain whether ASAM can enhance the agility and quality of Cyber SA.

Third, a host of experts suggest combining both qualitative and quantitative methods to exploit the possibilities offered by both (Creswell, 2003; Neuman, 2000). They also suggest adopting a method adapted to the nature of the investigation (Odell, 1998; Patton, 1990), where the method would not lead the research, but would instead be of consequence to the researcher's philosophical standpoint, since it "necessitates a philosophical solution to *why research*" (Holden & Lynch, 2002: 2). In the process, the researcher also learnt that the research method should emanate from logical deduction covering four issues: *epistemology*; *theoretical perspective*; *methodology*; and *methods* (Crotty, 1998).

The above views and assurances led this researcher to probe what epistemology (i.e. what theory of knowledge integrated into the theoretical perspective) should inform the research – objectivism or subjectivism – before exploring the philosophical perspectives of methodologies such as *positivism*, *post-positivism*, *interpretivism* and *critical theory*. In the process, Creswell (2003: 5) describes interrelated levels of decisions based on the above perspectives, which sets the research design in motion by virtue of three basic questions:

1. What knowledge claims are being made by the researcher (including which theoretical perspective)?
2. What strategies of inquiry will inform the procedures?
3. What methods of data collection and analysis will be used?

Creswell (2003) further defines his view through a diagram that depicts how three elements of inquiry, *knowledge claims*, *strategies* and *methods*, combine to form different approaches to research, before getting translated into processes in the design of the research:

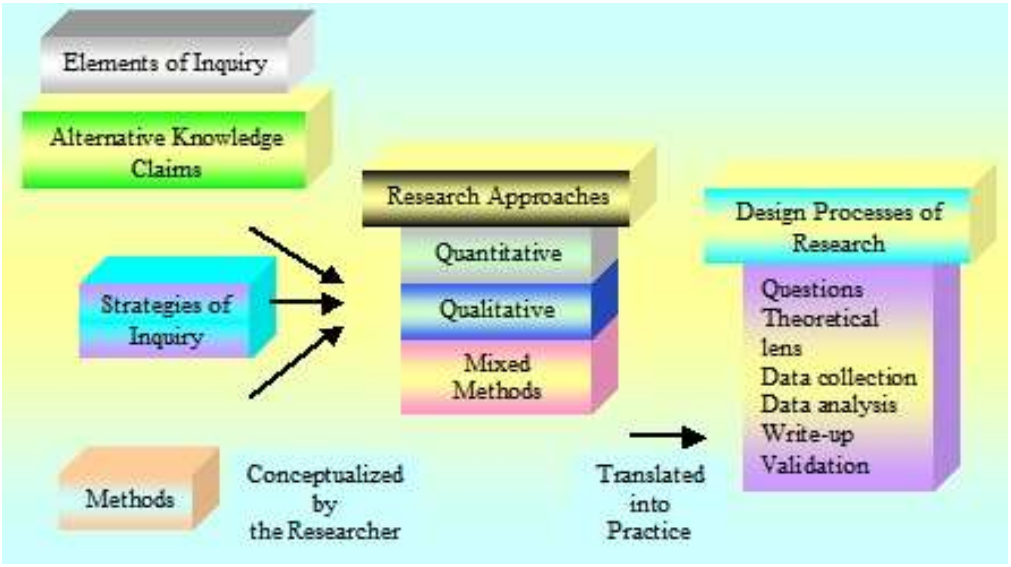


Figure 3.1: Knowledge Claims, Inquiry Strategy [adapted from Creswell (2003)]

The suggestions of Lincoln & Guba (2000) that stating a knowledge claim is actually the beginning of a research project, after which philosophical depiction of the same authenticates it, covering questions such as *what is knowledge* (ontology), how s/he knows it (epistemology), *what values are there* (axiology), *how s/he writes about it* (rhetoric), and *what processes s/he adopts to investigate* (methodology). This learning led the researcher to probe the four schools of knowledge claims, being *postpositivist*, *constructivist*, *advocacy/participatory*, *pragmatist*, *positivist and interpretivism* schools of thought. A brief account of the same appears below.

3.1.1 Types of Research Theories

This section provides an overview of the various theories and philosophies that are most relevant for the research methodologies considered. They are into two main groups: *natural science* and *design science*. The general concept is that natural science is concerned with explaining how and why things are, whereas design science is concerned with "devising artefacts to attain goals" (Simon, 1981). An in-depth summary of the corresponding theories is provided below.

3.1.1.1 Natural science research theories

March & Smith (1995) provide a very accurate and concise description: natural science includes traditional research into physical, biological, social and behavioural domains. Such research is aimed at understanding reality. Natural scientists develop sets of concepts, or specialised language, with which to characterise phenomena. These are used in higher order constructions – laws, models and theories – that make claims about the nature of reality. Theories – deep, principled explanations of phenomena (Achinstein, 1968) – are the crowning achievements of natural science research. Products of natural science research are evaluated against norms of truth, or explanatory power. Claims must be consistent with observed facts, the ability to predict future observations being a mark of explanatory success. Progress is achieved as new theories provide deeper, more encompassing and more accurate explanations.

Postpositivism: This challenges the traditional notion of absolute truth of knowledge (Philips & Burbules, 2000). This concept was shaped by eminent 19th-century scholars such as Comte, Durkheim, Locke, Mill and Newton (Smith, 1983). Postpositivists ask what warrants knowledge, which is also known as quantitative research. Socially constructed knowledge claims originated in the works of Berger and Luckmann; this school of thought claims knowledge through an alternative process and set of assumptions, and more often than not combines with interpretivism (Lincoln & Guba, 2000). According to this concept, individuals seek understanding of the world in which they live and work, and thus subjective meaning of experience should be developed to decipher the complexity of views. Accordingly, it mostly banks on the participants' views regarding the situation within a given context. Advocacy/participatory knowledge claims surfaced in the 1980s; this is a derivative of the works of Marx, Adorno, Marcuse, Babermas and Freire (Neuman, 2000), who observed that postpositivist

assumptions impose structural laws and theories that fail to fit marginalised individuals/groups. Thus, participatory knowledge suggests addressing social justice issues by containing an agenda for reform in the research that would change the lives of the participants, institutions or the researcher.

Pragmatism: This is an outcome of the works of Peirce, James, Mead and Dewey (Cherryholmes, 1992) that contains many forms. For example, a section of the pragmatists state that knowledge claims emerge from actions, situations and consequences, and that pragmatists express concern for the application and solution to problem (Patton, 1990). This concept assigns more importance to the research problem than to the research method. It also endorses the advantage of mixed method, and suggests focusing on the problem and then using a pluralistic approach to derive knowledge about the problem. Researchers like Cherryholmes (1992), Patton (1990) and Creswell (2003) observe that pragmatism claims knowledge on at least seven accounts:

1. It suggests adopting mixed method instead of adopting one single system of philosophy and reality, thereby enabling the researcher to draw inferences from both quantitative and qualitative methods;
2. It suggests freely choosing methods, techniques and procedures that would fit best fulfil research need and purpose;
3. It suggests employing several approaches to data collection and analysis;
4. It encourages researchers to exploit both quantitative and qualitative data to achieve best understanding of a research problem;
5. It looks into the *whats* and *hows* of research on the basis of its intended consequences, such as *where* they want to reach with the outcome. This also enables the researcher to justify the need to mix quantitative and qualitative data;
6. It accommodates the fact that research involves social, historical, political and other contexts that may appear relevant, besides accommodating the application of a theoretical lens through mixed method, which would reflect social justice and political aims;
7. It encourages achieving a change instead of questioning the reality, and for that matter it suggests including anything that is required to bring the desired change through research solutions.

The above suggestions made by the pragmatic school of thought appear best suited for this investigation, since this school too wanted to solve a problem (in the case of this research, presenting a comprehensive and viable cyber SA solution) and obtain a desired outcome (in this case, quality and agile cyber SA). At this point, the researcher realised that, within the context of this study, qualitative research could provide a deeper understanding of social phenomena involved with the research topic, and quantitative research could focus on collecting tangible proof on the same through SEM, where numerical data or structural representations would eventually accommodate or discard the findings of the qualitative research. Such a realisation was further consolidated with the views of Silverman (2000) and Ross et al. (2011), who identify mixed method's power to investigate the same research problem

from two directions, and thereby help the researcher to cover the diversities of the research topic. Such brainstorming eventually convinced this researcher of the utility value of mixed method within the context of the study.

The next task was to adopt an appropriate qualitative method and to formulate a logical sequence of research actions. Thus, the researcher reviewed the major three qualitative research approaches, *ethnography*, *phenomenology* and *grounded theory*, in order to select the right method.

First, the researcher found that the *ethnographic approach* emerged from cultural anthropology, and focuses on ethnic groups with emphasis on the nature, construction and sustenance of that culture. In the process it "attempts to explicate structured patterns of action that are cultural and/or social rather than merely cognitive, behavioral or affective" (Arnould, 1998: 86). It deals more with lifestyle investigation within a cultural or sub-cultural context (Stebbins, 1997).

Second, the researcher found that the *phenomenological approach* tries to create an understanding of complex issues that contain nuances that otherwise go unnoticed. For that matter, it enlarges and deepens the understanding of the range of immediate experiences (Shultz, 1967; Spiegelberg, 1982), and in the process it critically reflects on conscious experience rather than subconscious motivation, while unfolding essential and constant features of an experience. Altogether, it can be exploited to theorise the basis of lived experience (Merleau-Ponty, 1962; Jopling, 1996).

Third, the researcher found that *grounded theory* emerged from *symbolic interactionism*, which suggests that "[i]ndividuals engage in a world that requires reflexive interaction as averse to environmental response. Accordingly behavior is goal driven, evolving from social interaction that is highly symbolic itself" (Goulding 2005: 295). Such behaviour includes both verbal and non-verbal communication, where the notion of symbols appears intrinsic to the perspective (Schwandt, 1994). Symbolic interactionism was theorised by many researchers, such as Lazarsfeld, Merton, Hyman and Strauss, before Glaser developed a systematic and well defined procedure of the collection and analysis of qualitative data and named it grounded theory (Glaser & Strauss, 1967; Glaser, 1998), since it aims to generate a theory that would be grounded in the words and the actions of the individuals involved in the study.

The above descriptions of the three types of the qualitative research approach clearly highlight their differences in outlook as well as in procedures. For example, this researcher found the ethnographic approach falling short of the requirements of this study, which needs to cover elements that are spread across a heterogeneous setting in order to test the potential of the ASAM. Similarly, the phenomenological approach also appeared inadequate in this context, since this study aims to reach a definitive conclusion (i.e. whether ASAM can optimise quality and agile cyber SA), rather than describing the inherent elements of a situation and building a theory on it.

Positivism is a theory that aims to isolate concepts and phenomena, allowing a hypothesis and theory to be generated based on the results of the analysis and data collected. In turn, the concepts and hypothesis are then tested by generalising the study to fit a larger model and iteratively improve on the theory/model. Limpanitgul (2009) writes that positivist methods consist of observations, experiments and survey techniques, and often involve complicated statistical analysis in order to generate the findings and to test hypotheses empirically (Schiffman & Kanuk, 1997).

There is often a need to manipulate 'reality', with variations in only a single independent variable so as to identify regularities in, and to form relationships between, some of the constituent elements of the social world (Davison, 1998). Straub et al. (2004) reinforce the notion that the need to ensure that the data being gathered are as objective as possible, and a relatively accurate representation of the underlying phenomenon, is paramount. They go on to state that positivist science needs to be more than a series of anecdote or highly biased observations, where instead careful and thoughtful data gathering and intellectual constructs are needed. This research has developed the theoretical conjecture (Active SA hypothesised model) through examining literature where active SA theory then seeks the input and response of the community of cyber security subject-matter experts to collectively contribute to the building of active SA theory. Therefore, the positivist approach was adopted in this research because it is the most suited approach for this matter.

Researchers Alavi & Carlson (1992) have found that, although many authors have chosen to adapt a positivist approach in their respective papers, there is also a vast community of researches alike who believe there should be other methodologies and theories used (Kuhn, 1970; Bjørn-Andersen, 1985; Remenyi & Williams, 1996).
Interpretivists believe that reality is not objectively determined, but is socially constructed (Husserl, 1965), and is fully understood by studying it in its natural environment and formulating the concepts accordingly. By its nature, interpretivism promotes the value of qualitative data in pursuit of knowledge (Kaplan & Maxwell, 1994), leading the researcher to a better understanding of the concept/phenomena under study, which in turn allows generalisation of those 'understandings' to be tested on other phenomena. Kelliher (2005) states that, in essence, this research paradigm is concerned with the uniqueness of a particular situation, contributing to the underlying pursuit of contextual depth (Myers, 1997). From this discussion, it is clear that the only approach fit for this research is positivism. This research theoretical conjecture was developed based on literature, and then the theory of active SA had to consider how cyber security subject matter experts would respond to and collectively contribute to the building of this research theory. However, while interpretive research is recognised for its value in providing contextual depth, results are often criticised in terms of validity, reliability and the ability to generalise, referred to collectively as research legitimisation. These concerns are amplified in a single case scenario (Eisenhardt, 1989; Perry, 1998).

3.1.1.2 Design science research methodology (DSRM)

The theory of active SA requires an environment that allows applying the theory in practice while maintaining all legal constraints. Therefore, a serious gaming environment was developed for this research in order to examine the active offensive capability in enhancing the agility and quality of cyber SA to defend against cyber attacks. For this purpose, a design science methodology is required to build a SA assessment framework and a testing environment. The following will discuss the design science in detail.

Derived from March & Smith (1995), the argument follows that, whereas natural science tries to understand reality, design science attempts to create things that serve human purposes. Design science is technology-oriented. Its products are assessed against criteria of value or utility – do they work? Are they an improvement? Rather than producing general, theoretical knowledge, design scientists produce and apply knowledge of tasks or situations in order to create effective artefacts. If science is an activity that produces "credentialed knowledge" (Mishra & Eich, 1992), then, following Simon (1981), design science is an important part of it. Design science products are of four types: constructs; models; methods; implementations.

Design Science in Information Systems

Hevner and et al.'s (2004) design science principle for Information Systems (IS) has produced a seven-point guideline in which they write that knowledge and understanding of a design problem and its solution are acquired in the building and application of an artefact, shown below:

1. Design as an Artefact (Serious Gaming Environment) –

Design-science research must produce a viable artefact in the form of a construct, a model, a method or an instantiation.

2. Problem Relevance –

The objective of design-science research is to develop technology-based solutions to important and relevant business problems. In this research, Active SA capabilities are required to enhance cyber security.

3. Design Evaluation –

The utility, quality, and efficacy of a design artefact must be rigorously demonstrated via well-executed evaluation methods. The evaluation methods proposed can be broken down into the following groups:

a. Observational – via case studies (in business environments) or field studies (monitoring the use of the artefacts in multiple projects).
b. Analytical – examining the artefact for static qualities such as complexity, fit of artefact in technical architecture, demonstrated optimal properties of artefact, or its performance (dynamic qualities).
c. Experimental – either in a controlled experiment (for example: usability) or in a simulation where one can run the artefact with artificial data.
d. Testing – Black Box (test interfaces to artefact) or White Box testing (using metrics such as execution paths in artefacts implementation).

e. Descriptive – use of information from knowledge base to build argument for artefact's utility or in the form of scenarios.

In this research, several methods were used to evaluate the serious gaming environments, but mainly they were observational, experimental and testing. More detail about serious gaming environment design is discussed later in this chapter.

4. Research Contributions –

Effective design-science research must provide clear and verifiable contributions in the areas of the design artefact, design foundations, and/or design methodologies.

a. Design Artefact – the ability to reuse the artefact itself to solve other unsolved problems.
b. Foundations – to create new constructs, models, methods etc. to extend or improve existing foundations.
c. Methodologies – to produce new ways to evaluate and create new contributions to design science. An example is a framework for predicting and explaining why a particular information system will or will not be accepted in a given organisational setting (Venkatesh, 2000).

5. Research Rigour –

Design-science research relies upon the application of rigorous methods in both the construction and evaluation of the design artefact.

6. Design as a Search Process –

The search for an effective artefact requires utilising available means to reach desired ends while satisfying laws in the problem environment.

7. Communication of Research –

Design-science research must be presented effectively both to technology-oriented as well as management-oriented audiences.

With reference to the points above, Hevner et al. (2004) explain that, because the creation of an innovative, purposeful artefact (Guideline 1) for a specified problem domain (Guideline 2) is purposeful, the artefact must yield utility for the specified problem. Hence, thorough evaluation of the artefact is crucial (Guideline 3). Novelty is similarly crucial, since the artefact must be innovative, solving a hitherto unsolved problem or solving a known problem in a more effective or efficient manner (Guideline 4). In this way, design-science research is differentiated from the practice of design. The artefact itself must be rigorously defined, formally represented, coherent and internally consistent (Guideline 5). The process by which the artefact is created, and often the artefact itself, incorporates or enables a search process whereby a problem space is constructed and a mechanism proposed or enacted in order to find an effective solution (Guideline 6). Finally, the results of the design-science research

must be communicated effectively (Guideline 7), both to a technical audience (researchers who will extend them and practitioners who will implement them) and to a managerial audience (researchers who will study them in context and practitioners who will decide if they should be implemented within their organisations).

Hevner et al. (2004) conclude by recommending that design science should be paired with behavioural/natural science as well, since utilising design alone means taking a simplistic view of the people and the organisational contexts in which designed artefacts must function. In turn, they write that these must be combined with behavioural and organisational theories to develop an understanding of business problems, contexts, solutions and evaluation approaches adequate to servicing the IS research and practitioner communities.

Peffers and colleagues (2007) have produced another design science methodology for IS. Similar to Hevner and colleagues (2004) they have chosen to produce a six-point structure to aid the development of the DSRM methodology, shown below and referred to as 'activities'.

1. Problem Identification and Motivation –

Define the specific research problem and justify the value of a solution. Because the problem definition will be used to develop an artefact that can effectively provide a solution, it may be useful to atomise the problem conceptually so that the solution can capture its complexity. Justifying the value of a solution accomplishes two things: it motivates the researcher and the audience of the research to pursue the solution and accept the results, and it helps explain the reasoning associated with the researcher's understanding of the problem. Resources required for this activity include knowledge of the state of the problem and the importance of its solution.

2. Define the Objectives for a Solution –

Infer the objectives of a solution from the problem definition and knowledge of what is possible and feasible. The objectives can be quantitative, such as terms in which a desirable solution would be better than current ones, or qualitative, such as a description of how a new artefact is expected to support solutions to problems not hitherto addressed. The objectives should be inferred rationally from the problem specification. Resources required for this include knowledge of the state of any given problem, current solutions, if any, and their efficacy.

3. Design and Development –

Create the artefact (constructs, models, methods or instantiations, each defined broadly) (Hevner et al., 2004) or "new properties of technical, social, and/or informational resources" (Järvinen, 2007). Conceptually, a design research artefact can be any designed object in which a research contribution is embedded in the design. This activity includes determining the artefact's desired functionality and its architecture and then creating the actual artefact. Resources required for moving from objectives to design and development include knowledge of any theory that can be brought to bear in a solution.

4. Demonstration –

Demonstrate the use of the artefact to solve one or more instances of the problem. This could involve its use in experimentation, simulation, case study, proof or other appropriate activity. Resources required for the demonstration include effective knowledge of how to use the artefact to solve the problem.

5. Evaluation –

Observe and measure how well the artefact supports a solution to the problem. This activity involves comparing the objectives of a solution to actual observed results derived from using the artefact in the demonstration. It requires knowledge of relevant metrics and analysis techniques. Depending on the nature of the problem venue and the artefact, evaluation could take many forms. It could include items such as a comparison of the artefact's functionality with the solution objectives from Activity 2, objective quantitative performance measures such as budgets or items produced, or the results of satisfaction surveys, client feedback or simulations. It could include quantifiable measures of system performance, such as response time or availability. Conceptually, such evaluations could include any appropriate empirical evidence or logical proof. At the end of this activity, the researchers can decide whether to iterate back to Activity 3 to try to improve the effectiveness of the artefact, or continue on to communication and leave further improvement to subsequent projects. The nature of the research venue may dictate whether such iteration is feasible or not.

6. Communication –

Communicate the problem and its importance, the artefact, its utility and novelty, the rigor of its design, and its effectiveness to researchers and other relevant audiences, such as practicing professionals, when appropriate. In scholarly research publications, researchers might use the form of this process to structure the paper, just as the nominal structure of an empirical research process (problem definition, literature review, hypothesis development, data collection, analysis, results, discussion and conclusion) is a common structure for empirical research papers. Communication requires knowledge of the culture of the discipline.

Peffers and colleagues (2007) write that design science research comes from a history of design as a component of engineering and computer science research, while action research originates from the concept of the researcher as an 'active participant' in solving practical problems in the course of studying them in organisational contexts. In DS research, design and the proof of its usefulness are the central components, whereas in action research, the focus of interest is the organisational context and the active search for problem solutions therein.

The design science methodology was used in this research to design and build the SA assessment framework and the serious gaming environment to apply the active SA theory into practice. More detail will be provided, later, in the research experiment and ASAM testing environment section.

3.1.2 Types of Research Approaches

Fundamentally, there are two types of research approaches, inductive and deductive. Saunders et al. (2007) attribute positivism to deduction and interpretivism to induction, albeit with caveats, rendering such labelling potentially misleading.

3.1.2.1 Deduction vs. induction

From the very definition of deduction, and according to Saunders et al. (2007), this is the development of a theory that is subjected to a rigorous test. This ties in neatly with the research approach exhibited in natural sciences, where theorems and laws are built and tested against phenomena that might take the form of predicting their occurrences etc. In effect, it allows the researcher to test theories using the phenomena available. Therefore, this approach is adopted in this research so the active SA theories will be tested to understand why would active offensive intelligence gathering enhance cyber SA security and at the same time, find out how much better is the cyber SA.

Induction differs from deduction in the sense that it concerns itself predominantly with building theories from the data and information collected, whereas deduction focuses on building theories that the collected data can later be used to test and prove/disprove accordingly. In inductive approaches it is more effective to use smaller samples of data to build theories from, whereas the opposite can be said for deductive approaches.

Easterby-Smith et al. (2008) provide three key reasons why a distinction between the above two approaches is important: one of them is that, if the researcher is particularly interested in why something is happening, rather than being able to describe what is happening, it may be more appropriate to undertake the research inductively rather than deductively. Therefore, this research is intended to describe how to achieve better cyber SA through utilising offensive capabilities, so deductive approach is most suitable for this matter.

3.1.3 Types of Research Strategies

A paper by Davison (1998) breaks down the popular research methodologies, in addition to categorising them into our two major types of natural science research theories: positivism and interpretivism. The table can be found below.

Table 3.1: Taxonomy of Research Methodologies

Positivist	Interpretivist
• Lab Experiments	• Subjective/Argumentative
• Field Experiments	• Reviews
• Surveys	• Action Research
• Case Studies	• Case Studies
• Theorem Proof	• Descriptive/Interpretive
• Forecasting	• Futures Research
• Simulation	• Role/Game Playing

A Taxonomy of Research Methodologies (Davison, 1998).

Due to the nature of this research, survey and lab experiment strategies are the methodologies most suited to this research. This is due to fact that this study seeks to reach the community of cyber security subject matter experts from across the world to contribute in the development of active cyber SA theory. The following discussion is about different methodologies.

3.1.3.1 Surveys

Surveys (Davison, 1998) are a means of obtaining data via questionnaires and/or interviews. Multiple surveys can be conducted at different times in order to obtain an understanding of the individuals' opinions and views at various stages of the investigation, a process which subsequently provides the means to track changes. Surveys do not have to only be an open-ended collection of texts; they can also ask the target audience to rate/grade items, which in turn will allow for quantitative analysis to occur. Surveys can also be produced in such a way that similar questions can be reworded and restructured, allowing the producer of the survey to double-check the answers and opinions of the target audience. Davison (1998) the main advantage of survey is that it is a cost effective way of obtaining data from a large number of respondents located across the world. In this research, cyber security experts' contributions were really important, so a survey method was adopted. Another reason was efficiency: structure equation modelling would have required at least 200 participants, so the best way was to use an online questionnaire to reach the cyber security experts across the world.

A key weakness in surveying is that it is very difficult to realise insights relating to the causes of or processes involved in the phenomena measured. There are, in addition, several sources of bias, such as the possibly self-selecting nature of respondents, the point in time when the survey is conducted and in the researcher him/herself, shown through the design of the survey itself.

3.1.3.2 Case studies

Soy (1997) describes the case study as a way that emphasises detailed contextual analysis of a limited number of events or conditions and their inter-relationships in qualitative way. Its aim is to examine contemporary, real-life situations and provide the basis for the application of ideas and extension of methods. Soy continues to state that researcher Yin defines the case study research method as an empirical inquiry that investigates a contemporary phenomenon within its real-life context, when the boundaries between phenomenon and context are not clearly evident, and in which multiple sources of evidence are used (Yin, 1984). This shows that a case study cannot be adopted, as active SA requires cyber security experts around the world to contribute into building the active SA.

3.1.3.3 Action research

Davison (1998) has provided a compilation from various sources of what action research is; Elden & Chisholm (1993) go on to note that action research is change-oriented, i.e. seeking to introduce changes with positive social values, the key focus of the practice being on a problem and its solution. Thus,

Sanford (1970) views action research as a form of problem-centred research that bridges the divide between theory and practice, enabling the researcher to develop applicable knowledge in the problem domain (Peters & Robinson, 1984). Again, due to the nature of this research, action research cannot be adopted due to the fact that SA literature already exists, and this research problem has been identified while studying the literature.

3.1.4 Combining Natural and Design Science

It is really important to point that natural science is core in developing the theory of active SA, while design science in this research was used to develop the SA assessment framework and serious gaming environment to put the active SA theory into practice. Therefore, combining both sciences was crucial for this research, and this is based on the evidence discussed by March & Smith (1995), who have explicitly pointed out two critical points pertaining to the interaction between and combination of natural and design science, as shown below.

- Design science creates artefacts, giving rise to phenomena that can be the targets of natural science research. Group decision support systems, for example, foster user behaviours that are the subject of natural science investigations (George et al., 1988).
- Since artefacts "have no dispensation to ignore or violate natural laws" (Simon, 1981), their design can be aided by explicit understanding of natural phenomena. Thus, natural scientists create knowledge which design scientists can exploit in their attempts to develop technology. To conclude, March & Smith (1995) provide an example from the field of medicine whereby the explanation of why a drug is effective in combating a disease may not be known until long after the drug is in common use.

3.1.5 Techniques for Measuring Situational Awareness

It is really important to review the current methods used on evaluating SA for developing active SA theory. This is due to the fact that the measurement of SA is important to identify how good participant SA is, so that active SA can be measured and evaluated. According to the current literature, two SA-evaluation methods emerge as popular methods. The first of them is known as the Situation Awareness Global Assessment Technique (SAGAT), and the second is the Situational Awareness Rating Technique (SART).

3.1.5.1 SAGAT

As noted by Salmon et al. (2006), SAGAT is a freeze-probe technique, where random freezes are performed, blanking all screens and displays in a simulation, which is then followed by a list of SA-related questions. SAGAT requires all participants to answer each question based on their perceived SA, and a score is calculated at the end of the trial.

SAGAT provides an objective measure of SA for knowledge labelling in manned simulations of the task environment, where it directly compares operators' reported SA to reality. SAGAT intervenes in a human in-the-loop simulation at specific times, and queries the subjects by using a computerised tool for determining their current understanding of the situation at that particular point in time. In this case, SAGAT compares the answers of the subjects with the correct answers, which are simultaneously collected through the simulation computer. Such comparisons between real and perceived situations provide an objective, unbiased assessment of SA. Its random sampling method also ensures its validity and reliability.

SAGAT queries require covering all levels of SA, such as perception, comprehension and projection, to provide an accurate measure of the operator's SA, besides covering and reflecting on the wide range of the operators' SA requirements, which are delineated through a goal-directed task analysis, which in turn identifies the operators' goals, the decisions the operators must make to achieve those goals, and the information needed by the operators for decision making. The necessary information is the operators' SA requirements, which form the basis for the development of the SAGAT queries.

Various studies have tested SAGAT, in various forms, a fact that demonstrates its empirical validity (Endsley, 1989a, 1989b), predictive validity (Endsley, 1990a) – by linking its scores to subject performance – and content validity (Endsley, 1990b) – by exhibiting the appropriateness of the queries. The proven efficacy of SAGAT, therefore, automatically qualifies it as the tool to measure the efficacy of ASAM.

3.1.5.2 SART

SART provides a subjective measure of SA, and is capable of providing a critical link between SA and performance by measuring a person's perceived quality of SA. However, Endsley's (1990a) research findings point to the fact that it may not be possible to validate SART findings, since subjective and objective measures of SA cannot be correlated.

Salmon et al. (2006) note that SART attempts to measure how aware a participant perceives himself or herself to be during the task, and does not refer to the different elements within the environment. Whilst questions on SAGAT might be similar to: "How many buildings did you notice", a SART question would be along the lines of: "How changeable was the situation?" or "How much information did you gain through this trial?" all within a scale (e.g. 1-7).

SARTs are usually carried out post-trial, and involve participants providing a subjective rating of their perceived SA via a rating scale. This differs to the interruption-based technique of SAGAT.

3.1.5.3 Comparison of SAGAT and SART

Table 3.2: Differences between SAGAT and SART

	SAGAT	SART
Technique	Freeze Probe Technique	Self-Rating Technique
Performing the Measurements	Simulations paused at random intervals, screens blanked and questions asked. Answers validated against actual, pre-determined results of simulation.	Tests/questionnaires are carried out post-experiment.
Advantages	• Covers all levels of SA such as perception, comprehension and projection) • Removes issues associated with post-trial data collection	• Easier to carry out SARTs • Non-intrusive (carried out at end of test and not in between like SAGAT)
Disadvantages	• Intrusion on task performance (during the freezes), which does not happen in real-world scenarios • Questions are asked on items that the participant might not have been aware of in the first place	• Difficult to correlate SA with performance, such as the potential for poorly recalling the events
Outcomes	• Produces a score of participant's ability to recall elements in the environment, their associated properties and how they are likely to act in the future.* • SAGAT therefore compares participant SA against a normative ideal *	• Produces a score of how aware participants felt they were during task performance * • SART on the other hand makes no reference to any ideal, it merely tells us how aware participants felt they were *

Differences between SAGAT and SART SA measurement techniques. * = Salmon et al. (2006)

3.1.6 Assessing Situational Awareness

Situational awareness is regarded as a fundamental concept in the field of human factors practice and research, with the impacts of ever-increasing situational and technological complexity on the human agent recognised as a pivotal concern. As a result, valuable and meaningful SA measures are needed in order to evaluate the effects of new training methods, system designs and more. However, the question is then posed as to how an individual's SA can be assessed, as well as on what scientific basis it can be stated that an individual has a greater SA than another. On the other hand, how can it be suggested that a new data system has resulted in decision-makers demonstrating greater SA than previously? Importantly, SA evaluation is complex, which owes, in some regard, to the multifaceted nature of SA, as well as to the critical problems associated with observing and assessing what goes on in the mind of another individual.

Over the last ten years, a number of different approaches have been introduced with the purpose of examining and evaluating situational awareness. Ultimately, these techniques boil down to three of the most commonly acknowledged, which may be identified in line with the types of evidence seeking to be established:

Inferential techniques aim to garner implicit SA-related evidence through observable correlates, with the behaviour, performance and physiology of an individual monitored as indirect evidence for the absence or presence of suitable SA. For instance, through the use of the SALIANT approach, it is suggested by Muñiz et al. (1998) that a team's SA can be inferred through observed behaviours. Notably, the somewhat different SABARS (Situational Awareness Behaviourally Anchored Rating Scale) approach necessitates the involvement of professional observers with the objective of rating people according to various observable behaviours linked with SA processes (Strater et al., 2001). Although this is an unobtrusive approach, the restriction is that a performance error or SA-related behaviour omission does not ultimately suggest a lack of SA, whilst good performance does not necessarily suggest good SA (Baxter & Bass, 1998). A particular type of measurement intervention is commonly fundamental in attaining a good understanding of the SA of a person.

Self-rating approaches aim to gather subjective proof of SA through insight into the self-perceptions of people. Such techniques are embodied in a number of tools, including the Participant Situation Awareness Questionnaire (PSAQ) used by Matthews et al. (2000), the Situational Awareness Rating Tool (SART) of Taylor (1990), and the Crew Awareness Rating Scale (CARS) presented by McGuinness & Foy (2000). These instruments differ in the number of scales utilised and the dimensions rates. SA self-ratings can be gathered immediately following an experimental run or exercise, or can also be gathered one or more times mid-run with comparatively minimal disturbance.

Probe approaches or **query approaches** aim to gather direct evidence of the person's SA content. These techniques involve extracting different data from the person relating to their understanding and viewpoints of the situation, and accordingly draw comparisons with this and the actual truth. There are two main types of probe. First, with supply probes, the person is asked to provide particular data relating to the situation; second, with labour-intensive probes, accurate data are presented to the person, in addition to a number of incorrect alternatives, with the individual asked to choose the correct one. The second approach adopts a multiple-choice format, as in the case of the Situation Awareness Global Assessment Technique (SAGAT) of Endsley (1995, 2000). Such a technique is recognised as being the most disruptive and intrusive, but ultimately creates an abundance of direct evidence relating to an individual's SA state.

Nevertheless, this study aims to establish the most significant effects of derived intelligence through utilising offensive approaches in the participants' overall SA. Accordingly, the most suitable technique for such a study involves the application of a non-intrusive probe method, which helps to ensure the researcher captures all data necessary in order to evaluate the intelligence and draw a comparison with participants' SA. The tool has been validated, as shown in this chapter, in light of the suggestions made by Churchill (1979) and McDaniel & Gates (2006: 224-227), where semi-structured questionnaires, complete with open-ended questions, were prepared for this part of the project, as will be elaborated on later in this chapter.

3.1.7 Structural Equation Models (SEM)

In order to test and estimate causal relations of active SA hypothesised model and theory, this research utilised SEM. The reason behind utilising SEM is that SEM tests and estimates causal relations using combinations of statistical data and qualitative causal assumptions. Also, SEM's stages, which will be described in this chapter, are the most suited for both theory testing and theory development. This research has conducted surveys across cyber-security subject-matter experts in CERT teams around the world so the hypothesised model produced can be tested using SEM. The following section discusses SEM in general, where detailed discussion will be covered later in this chapter in the quantitative data analysis section.

Structural equation modelling (SEM) is a general statistical modelling technique widely used in behavioural sciences. From a broader perspective, it can be viewed as a combination of path analysis or regression and factor analysis as special cases of SEM (Steiger, 1987). It is a linear, cross sectional, statistical modelling technique. SEM is widely used by researchers to determine whether a given model is valid, and also in finding a suitable model in analysis. This often involves certain basic elements. Major interest in SEM focuses mainly on theoretical constructs, which are represented by latent factors. Path coefficients or regression between factors represent the relationship between theoretical constructs.

SEM refers to the structure for the covariance between the observed variables. This provides an alternative name: covariance structural modelling (MacKinnon, 2008). In some cases, the model is extended to include means of factors in the model or observed variables. This results in covariance structure modelling having a less accurate name. Some researchers simply take these models as Lisrel-models, which is less accurate as well. LISREL (linear structural relations) were used by Joreskog in one of the initial popular SEM programs. Currently, the research field, structural equation models are not necessarily required to be linear, while the possibilities of SEM extend far beyond the original LISREL program. Researchers such as Steiger (1987) have discussed the possibility of fitting nonlinear curves.

The most recent development in this field is software that allows researchers to specify the model directly as a path diagram. However, although this works extremely well for simple problems, it becomes really complex with complicated models. In this regard, current SEM software supports the command or matrix style model specifications as well.

3.1.7.1 Advantages and disadvantages of SEM

Table 3.3: The Advantages and Disadvantages of SEM (Author)

Advantages	Disadvantages
• **Validity** SEM allows making use of several indicator variables per construct simultaneously; this results in more valid conclusions on the construct level. • **Reliability/measurement of error** SEM takes measurement of error into consideration by explicitly including measurement error variables that match the measurement error portions of observed variables. • **Complex models** SEM allows the researcher to model and test complex patterns of relationships, including a multitude of hypotheses simultaneously as a whole, including mean structures and group comparisons. • **Confirmatory approach** SEM allows the researcher to test complex models for their compatibility with the data in their entirety; this allows testing specific assumptions about parameters, such as whether they equal zero or if they are identical to each other, for their compatibility with the data.	• **Model identification/parameter identification** It is not possible to estimate more model parameters than there are distinct entries in the empirical covariance matrix. • **Estimation methods and estimation challenges** The algorithms might not converge; this will result in no optimal solution being found. • **Assumptions, single size and distributions** Combining small sample sizes, non-normal data and weak empirical relationships between variables can lead to estimation problems and unreliable results. • **Interpretation of results** Decision problems may occur especially when there are two or more alternative models, making essentially different assumptions about the variables in causal relationships, but still leading to exactly the same model. This makes it hard to base a decision merely on statistical criteria (Schermelleh-Engel, 2009).

Advantages and Disadvantages of SEM

3.2 RESEARCH METHODS

Data were collected in this research using a combination of methods. Social sciences have provided evidence for the efficiency of using mixed-methods (Creswell, 2003) in a way that the reliability and validity of a construct is improved (e.g. Creswell, 2003; Churchill, 1979). It has been put forward by Morgan (1999) that when quantitative and qualitative methods are used simultaneously in the same research, their respective strengths are enhanced. These research approaches are considered to be at the two opposite extremes of the inquiry methods continuum (Krathwohl, 1997). The universal relationships of cause and effect between variables are verified through quantitative research. Educated estimations or hypotheses are formed by such research, after which they are used to analyse the data. A deductive approach is usually adopted by quantitative methods where development is guided by the explanation; the focus is chiefly on the statistical significance of the outcomes that have come about through empirical tests (Maykut & Morehouse, 1998). The purpose of qualitative research, on the other hand, is to identify meanings and patterns; the words of people, their actions and records are also closely examined. An inductive approach is normally adopted by qualitative research where data lead to explanation, which comes about through detailed observation and examination of the theme of the research (Rubin & Rubin, 1995). The quantitative approach is inclined towards positivist epistemology, while the qualitative method prefers a constructive/interpretive epistemology (Krathwohl, 1997). Qualitative data are considered by the positivists to be corresponding instruments that strengthen and illuminate the statistics that have been attained through the research instruments (Coolican, 2004). In addition, there are several possibilities, according to Bryman (1998), for using a qualitative method to test theories in a way that is normally associated with a positivistic approach (Myers, 1997).

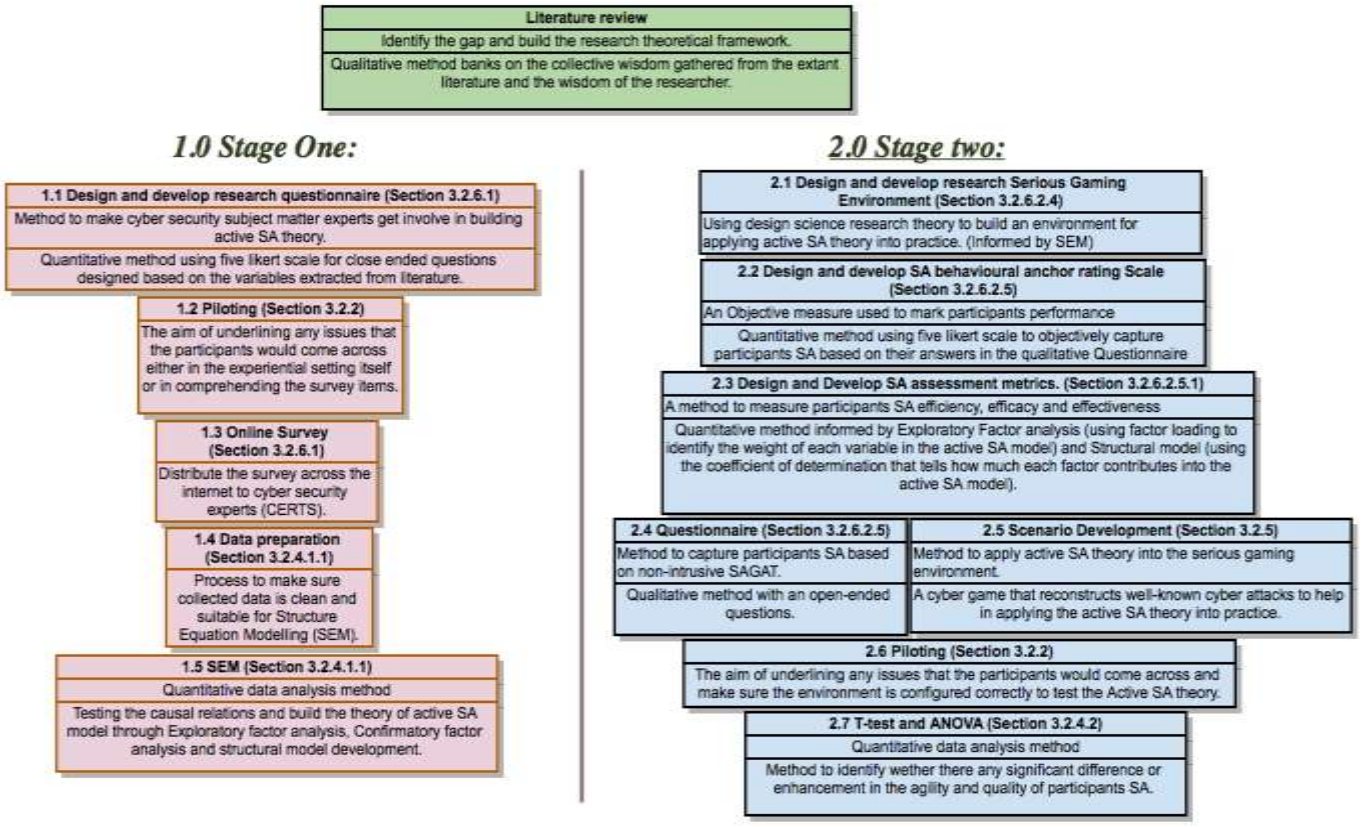
Several researchers are in favour of using multiple research methodologies in the field of information systems research (Galliers, 1992; Hirschheim, 1992; Winfield, 1990; Straub & Carlson, 1989). Galliers (1992) asserts that the domain of information systems is fundamentally a pluralistic scientific domain which "can best be understood and analyzed only with the help of pluralistic models" (148). According to Winfield (1990), information systems are considered to be systems of social communication that are ingrained in a cultural context. This is why various perspectives and explanations need to be considered when studying this field, hence the need to use multiple research techniques. Krathwohl (1997) believes that an essential aspect of social science research is using a mix of qualitative and quantitative techniques. He is of the view that not only can the weaknesses of a single method be compensated for through the use of a combination of methods, but diverse perspectives and details can be attained in this way.

Based on the explanations presented above, the thesis under discussion uses a mixed approach that combines both quantitative and qualitative methods. This consists of employing different instruments of data collection. This research adopts positivism deduction as its research approach, while opting for mixed methods to avail of its proven advantages in the area of information systems. Altogether, the study manifests through two stages, where in the first stage it collected data using electronic survey, which was quantitative in nature, while in the second stage it used the results of the survey to design and develop the qualitative and quantitative instruments to test the effectiveness, efficacy and efficiency of active SA. Accordingly, Structure Equation Modelling (SEM) was used in the first stage to verify the theoretical model and test the causal relation, and its outcome was then used in the second stage to design the serious gaming environment, SA awareness behavioural anchor rating scheme and SA measurement and marking scheme, based on ground truth.

The design science loop is related to the iterations followed in the development of the ASAM artefacts. The first iteration was the development of the hypothesised ASAM model based on the literature review. The second iteration was concerned with building a statistically significant theoretical model (i.e. the ASAM theory), using structural equation modelling (SEM), based on a survey of Cyber security experts. The third iteration was the practical validation of the ASAM theory and the development of the ASAM derived SA assessment framework by employing the Cyber range in serious gaming experiment where Cyber security practitioners, drawn from a sample frame of international CSIRTs, were used to assess the practical value of the emergent design science research artefacts i.e. the ASAM theory and its concomitant SA assessment framework.

In the second stage, the study adopted Independent Sample T-test to underpin the differences between Active and Passive conditions, as well as to underpin the differences between military and non-military background conditions. Alongside, One-Way ANOVA was used to underpin the differences between the control group (Blue Team) and the participants regarding utilisation of the deception in real-time cyber situation. Figure 3.2 outlines this research method and instrument and summarised the coming section in this chapter.

Figure 3.2: Research Method Outlines (Source: Author)



3.2.1 Sampling Techniques

This study utilises a non-random sampling approach, referred to as a convenience samples. It is suggested by Bryman & Bell (2007: 198) that "convenience samples are very common and indeed are more prominent than are samples based on probability sampling". Such an approach has been selected for this research owing to the fact that it has sought subjects' permission prior to survey completion. Upon the agreement of the subjects to take part in the survey, the research was initiated; if they wished to pull out, the research would stop and other subjects would be sought out.

3.2.1.1 Appropriate number of participants

In a sample size, the most suitable number of subjects is a complicated and not always straightforward decision. Accordingly, the decision was made that the research would adopt the most commonly adopted approaches when establishing the most suitable number for a sample. Importantly, the suggestion is typically made that researchers should follow pre-defined rules when establishing the most suitable sample size. In this regard, Roscoe (1975) provides four different rules of thumb for use when establishing the most suitable sample size (N).

- The number of participants should be smaller than 500 but greater than 30.
- If there is more than one group to be involved in the study, the suggestion is made that each group utilise more than 30 subjects.
- When utilising multivariate analyses, researchers are advised to utilise a larger sample, which is at least 10 times that of the number of variables adopted in the analysis. Moreover, it is further implied by Stevens (1996) that 15 cases per construct be utilised in order to calculate the most suitable sample size. In addition, researchers are advised that the sample size be established in regard to the number of parameters in place (Bentler & Chou, 1987). Importantly, if the data are distributed normally, at least five cases per parameter are considered suitable.
- If a simple laboratory experiment is to be carried out, and where various conditions are to be controlled, the most appropriate sample size should range between 10 and 20 subjects, as suggested by Roscoe (1975). A number of other academics, such as Krejcie & Morgan (1970), for example, suggest the use of a table in order to establish the most suitable sample size (S) derived from a population (N).

The second approach adopted by academics when establishing the most appropriate sample size rests on the data analysis approach to be implemented (Hair et al., 2006). With this taken into account, the research describes the five considerations Hair et al. (2006) suggest when establishing the proper sample size when utilising Structural Equation Modelling (SEM) methods. Primarily, these scholars highlight that, if the data distribution diverges from the multivariate normality assumption, the proportion 15 individuals for every parameter is considered a suitable number; this will help to reduce the issue associated with straying from the norm. Secondly, the sample size should be in the range of 150-400 subjects when there is the application of the estimation technique. To put it another way, SEM is centred on the MLE (Maximum Likelihood Estimation) approach, which provides suitable results if 150-400 subjects are used. Thirdly, there is the consideration of model complexity, which centres on the number of constructs to be adopted in the analysis; otherwise stated, a larger number of parameters should be utilised in the analysis when the model has a larger number of constructs, meaning a greater sample size would be required in order to complete the analysis. Furthermore, as highlighted by Hair et al. (2006), if a researcher adopts a multi-group analysis, a suitable sample size for each group is necessary. Fourthly, it is emphasised by the same researchers that a larger sample size is required when there is more missing data. In addition, the suggestion is made that commonalities need to be considered prior to establishing the size of sample to be utilised. Importantly, commonalities need to be in excess of .5 (Hair et al., 2006: 741) (equals .7 standardised loading estimates); if this is not ensured, a greater sample size would be necessary. For example, it is suggested by Hair et al. (2006) that, if any commonality is found to be between .45 and .55, or if the model comprises constructs with fewer than three items, the sample size would then need to be more than 200. Conversely, if commonalities are found to be below .45, the minimum sample size should then be more than 300.

In addition, researchers Durso et al. (1999), Endsley et al. (1999), Endsley & Garland (2000) and Salmon et al. (2009) measured SA performance using sample size range from 8-20 participants. This is due to the fact that the targeted sample in their studies was highly specialised personnel, where a small group can represent the whole population. This study, as described in the sample frame, uses highly specialised cyber security and cyber defence experts with not less than two years' experience. Due to this requirement, the sample size for the lab experiment in this research is similar to what has been adopted in previous researches. Also, according to Chow et al. (2003) and Rosner & Bernard (2011), the required sample size can be estimated using the formula given below.

$$n = \left(\frac{Z_{1-\beta} + Z_{1-\alpha/2}}{\mu_0 - \mu_1}\right)^2 . \sigma^2$$

n: The sample size.
$Z_{\alpha/2}$: The critical value.
σ: The standard deviation.
μ_1: The mean.
μ_0: The estimated mean.
α: Significance level (1 - degree of confidence (1- .95 = 0.05)).
$1 - \beta$: The power for detecting significant difference (power = 80%).
Applying this equation using the data found from the pilot, the result is:

$$n = \left(\frac{.84 + 1.96}{93 - 67.93}\right)^2 . \ 26.007^2 = \left(\frac{2.8}{25.07}\right)^2 . \ 676.3640 = 8.436996 \approx 9 \ participants$$

In consideration of the discussion provided above, and in mind of the fact that this study is centred on the utilisation of SEM, T-Test and ANOVA, this research utilised a sample size of more than 200 for the first stage to get the structural model, and a sample size of 20 or more for the lab experiment session.

3.2.2 Targeted Population and Piloting

The primary survey was circulated among a number of different cyber security firms for piloting, with 30 professionals in this arena targeted by the study. Notably, the researcher utilised the means and resources of the university and its contacts in order to generate the sample of cyber security organisations. Moreover, the survey was sent to a number of different reputable security businesses in the field, including UK-Cert, UAE-Cert and UK cyber securities firms, as well as various EU cyber security organisations and governmental entities. A number of other firms were Italian cyber security firms, UAE governments' cyber security organisations and the US-Cyber Security Institute (US-Cert), as well as firms operating in various other countries, including Australia, Germany, India, the Netherlands and Singapore.

The observations detailed below were made.

- The key respondents were professionals and experts in the field of cyber security, and all had at least 3 years' experience in the arena.
- The survey detailed questions linked with personal data; in other words, questions were demographic in nature.

- Sensitive questions were directly associated with active and offensive approaches, and other questions sought to determine whether businesses implemented such approaches.

3.2.2.1 Piloting

Piloting was carried out on the experiential session with the aim of underlining any issues that the participants would come across either in the experiential setting itself or in comprehending the survey items. The significance of piloting with respect to estimations of the time needed for the entire process, examination of any possible problems, and assessment of the reliability and consistency of survey items has been emphasised by McDaniel & Gates (2006) and Hair et al. (2006). Pilot testing was carried out on the two experiential survey sessions of this research with 30 participants at the first stage and 10 at the second stage, all of whom were part of cyber security and cyber incidents response. Those participating in the piloting phase were encouraged to give their feedback on the procedures, tasks and the survey.

The pilot questionnaire established that a significant number of respondents in the stage one survey did not want to be involved owing to the sensitive questions posed. Equally, some questions were believed to provide researchers with the opportunity to access firms' profile information, which could put them in a vulnerable position in terms of exploitation.
In mind of the factors highlighted above, the decision was made by the researcher to remove demographic questions, as well as any questions that probed whether firms implemented certain methods, from the first survey.

3.2.3 Purifying Measures

The framework introduced by Churchill (1979) seeks to purify the measurement scales by confirming and validating the overall reliability associated with each of the scale items. As has been highlighted by McDaniel & Gates (2006: 224-227), validity is explained as being "the degree to which what the researcher was trying to measure was actually measured". With this noted, this paper has carried out two different validation approaches through the use of a main survey and lab experiment survey: content validity and face validity. In contrast to these, however, reliability is defined by the aforementioned scholars (McDaniel & Gates, 2006: 222) as being "the degree to which measures are free from random error and, therefore, provide a consistent data". In this regard, this paper calculates the reliability test through the use of Cronbach's Alpha, which should be at least 0.70 (Hair et al., 2006). Through the adoption of reliability and validation instruments, as considered above, the ways discussed below have purified the scales.

3.2.3.1 Qualitative assessment

Throughout the qualitative assessment approach, the research has examined two different forms of validity, namely content validity and face validity. Markedly, scholars McDaniel & Gates (2006) explain content validity as being "the responsiveness, or sampling adequacy, of the content of the measurement instrument" (225), whilst face validity is highlighted as "the degree to which a

measurement seems to measure what it is supposed to measure" (225). Both approaches have been utilised for all constructs through the submission of the items for assessment by the academics and professionals in the arena of cyber security. The sample considered the questions appropriate for construct measurement, and adequate in this regard for both instruments used in this research.

3.2.3.2 Quantitative assessment

During the examination of the pilot study (Stage one n = 40) and (Stage two n = 10), Cronbach's Alpha reliability and factor analysis was carried out in regard to each construct alone. Cronbach's Alpha has been found to provide a value of in excess of 0.8 for all of the constructs, which is notably above the suggested threshold of 0.7 recommended by Hair et al. (2006).

3.2.3.3 Justification for using a 5-point Likert scale

A 5-point Likert scale is adopted for this research. It is common for such a scale to be utilised, as it facilitates the simple gathering of data from subjects through the use of a survey (Preston & Colman, 2000; Sekaran, 2000). Importantly, the rationalisation behind utilising such a scale has been debated widely (Cox, 1986). For instance, it is held by some that a scale utilising seven, nine or sometimes more points is preferable, whilst others believe a lower number is more acceptable. Importantly, a greater number of points on the scale means greater validity and power of discrimination (Preston & Colman, 2000). On the other hand, however, a response rate is usually greater when five points are utilised (Hartely & Mclean, 2006). Furthermore, the empirical research carried out by Dawes (2002) highlights a change in validity and reliability when there is the use of a seven-point scale when compared with a five-point scale. In this vein, Dawes (2002) suggests that such a Likert scale will produce greater validity and reliability. Furthermore, Dawes also emphasises that, when implementing an 11-point Likert scale, the same mean is achieved as when a 5-point scale is adopted. Furthermore, kurtosis and skewness are seen to show unsystematic differences. With this in mind, it is noted by Neumann (1983) that the use of a 5-point and 11-point Likert scale provides comparable findings, such as in relation to the correlation coefficients and means. Furthermore, the author suggests that a 5-point Likert scale be utilised when attitudinal studies are being conducted.

3.2.4 Quantitative Data Analysis Techniques and Statistical Packages

Owing to the fact that a mix of data-gathering approaches are utilised throughout the course of this study, it should then be recognised that both quantitative and qualitative strands of analysis have been adopted. The key quantitative data analysis was carried out through the use of the SEM (Structural Equation Modelling), whereas an analysis was utilised with qualitative analysis in mind, and participants involved in filling 4 SA questions using SAGAT technique; then, based on their answers, participants were marked objectively using the research scale, so that independent sample T-Test and One way ANOVA could be used to analyse the findings. This section considers the application of such methods throughout the two study stages.

An SEM was carried out through the use of a statistical software package developed by IBM called Statistical Package for Social Sciences (SPSS), version 20.0. SPSS was adopted for primary data analysis, with SEM adopted in order to test the structural model and measurement model. In addition to this, a modular add-on to SPSS, referred to as AMOS (Analysis of Moment Structure) version 20.0, was employed with the aim of establishing the goodness-of-fit of indexes associated with the suggested framework, and to test the hypotheses suggested in the ASAM framework. It is designed primarily for SEM, path analysis and covariance structure modelling. (University of Texas at Austin, 2010).
The use of these statistical packages allowed for better management of the data and the ability to handle large amounts of data that could be imported directly from Excel and other spread sheets. The appropriateness of utilising SPSS has been recognised and verified by a number of different academics (Field, 2005; Tabachnick & Fidell, 2007), and SPSS was adopted in this research for various reasons, namely for coding, checking missing data and editing, as well as for checking the assumptions of linearity, multicolinarity, normality and outliers. Greater detail about the tests can be seen in Chapter 4.

3.2.4.1 Structural Equation Modelling (SEM)

SEM was adopted with the aim of testing the causal relations outlined in the ASAM framework. In line with the view of Tabachnick & Fidell (2007: 676), SEM is described as being a "collection of statistical techniques that allow a set of relationships between one or more independent variables, either continuous or discrete, and one or more dependent variables, either continuous or discrete, to be examined". SEM is an approach that aims to highlight the data gathered in regard to various structural parameters, namely those defined through a hypothesised, underpinning framework. Essentially, SEM is considered a theory-based approach, which has the capacity to amalgamate theory and data (Tabachnick & Fidell, 2000). Moreover, SEM is recognised for its capacity to conduct simultaneous analysis, where the links between dependent and independent constructs are modelled simultaneously. This capacity varies significantly from the majority of first-generation statistical measures such as correlation, factor analysis and regression, which have the ability to examine at any one time only one layer of linkage between dependent and independent variables (Chin, 1998). Importantly, SEM has enabled social scientists to carry out path analytic modelling with latent variables; subsequently, this has resulted in this approach being described as an example of a second-generation form of multivariate analysis (Hair, Anderson, Tatham & Black, 1998).

The causation between independent and dependent constructs, namely Structural Modelling Analysis, is not examined by SEM as a sole activity; rather, SEM also assesses measurement loadings in regard to their expected constructs (measurement model analysis). Accordingly, in the context of SEM, hypotheses and factor analysis are tried and examined in the same stage. In line with the work of Gefen et al. (2000), the combined analysis and measurement of the structural model facilitates the observed variables' measurement errors to be examined as a key aspect of the framework, in addition to the combination of factor analysis in one operation alongside hypothesis testing. The result is a more exact and precise analysis of the research hypothesised model suggested, with an overall improved methodological assessment established afterwards (Bollen, 1989).

Unsurprisingly, SEM tools are becoming more and more widely utilised in the context of behavioural science studies for the causal modelling of complex and multivariate data sets where the research gathers a number of different measures for the proposed constructs (Hair et al., 1998). In the view of Gefen et al. (2000), an informal review of the IS literature suggests that SEM has become recognised widely in terms of assessing and verifying tools and examining the links between constructs. Moreover, a significant increase in SEM utilisation has become recognised widely in IS journals. In contrast, however, SEM analysis's application in the IS domain has increased significantly, owing to the availability of various software packages with the capacity to carry out SEM, namely AMOS, LISREL and PLS-Graph (Chin, 1998).

The adoption of the SPSS and SEM for this research was a decision made on the basis of various factors, and by considering the works of Hair et al. (2006) and Tabachnick & Fidell (2007). Primarily, the simultaneous capacity of SEM to test a number of different dependent links between the latent variable and observable indicators, as well as to test the links between latent variables is better when contrasted alongside other statistical packages, such as SPSS, with many analysing only one link at any one time. Second, SEM has the capacity to assess the reliability, unidimensionality and validity of each construct on an individual basis. Third, SEM has the capacity to test the confirmatory factor analysis as opposed to the exploratory factor analysis, which adds a further benefit. Fourth, SEM is able to predict the total indirect and direct effects, which means SEM has a number of advantages over other statistical packages. Finally, in contrast with other multiple variance approaches, SEM is able to calculate error variance and measurement error parameters, and delivers a generalised goodness-of-fit for the models tested.

3.2.4.1.1 Stages in Structural Equation Modelling

This study has incorporated three different phases for the analysis of SEM data. Primarily, the thesis has been initiated through examining the measurement model for all of the constructs; in other words, calculating confirmatory factor analysis. This action has been adopted for two different reasons:

1. To ensure that the link between every unobserved construct and its observed items has attained the unidimensionality assumption. Throughout this phase, CFA (Confirmatory Factor Analysis) was adopted in order to ensure standardised factor loadings values would be more than .60, which is known to imply a significant link between the items and their respective construct (Hair et al., 2006).
2. To perform a calculation to determine each construct's reliability and validity. Although this research is conducted through the use of EFA (exploratory factor analysis), CFA is viewed as being more valuable than EFA (Hair et al., 2006).

Notably, a structural framework is adopted in order to test the casual or hypothesised links between any concealed constructs. Critical ratio values, namely t-values, are adopted in order to establish the importance, or lack of importance, associated with the links between the unobserved (latent) constructs.

Goodness-of-fit criteria and unidimensionality were adopted with the aim of assessing the measurement framework along with its specifications. In one regard, there was the evaluation of unidimensionality through reliability tests, namely Cronbach's Alpha reliabilities and composites, and factor loadings for all of the constructs – but each in isolation. In contrast, a number of goodness-of-fit criteria have been selected in this study, owing to the fact that it is difficult to rely on a single-fit index when seeking to establish the best model (Byrne, 2001). This paper has directed attention to three different forms of goodness-of-fit, namely absolute fit indices, incremental fit indices and parsimony fit indices.

First, in the view of Hair et al. (2006: 706-708), absolute fit indices are utilised with the aim of measuring "the overall goodness-of-fit for both the structural and measurement models collectively". Furthermore, these indices suggest the extent to which "the hypothesised model reproduces the sample data" (Shah & Goldstein, 2006: 159). In short, absolute fit indices independently assess the goodness-of-fit associated with a certain model distinct from any other model. This paper has adopted the absolute fit indices shown below.

1. The chi-square ($\chi 2$) test is linked with the "fit between the sample covariance matrix and the estimated population covariance matrix", as recognised by Tabachnick & Fidell (2007: 715). The notable differences between the matrices should not be seen to be the same statistically ($p > .05$). Nevertheless, adopting such a fit in order to evaluate the overall goodness-of-fit framework has been the focus of much criticism, owing to the fact that sample size has an impact on chi-square (Hair et al., 2006; Tabachnick & Fidell, 2007). Accordingly, in order to quantify the degree of fit, a number of academics have neither accepted nor rejected a framework considering only the $\chi 2$ value, but rather utilise a mix with other indices.
2. GFI (Goodness-of-Fit Index) is concerned with the measurement of the appropriate amount of covariance and variance in the sample matrix, and is described jointly through a population matrix (Byrne, 2001, p. 82). The values of GFI span 0-1, with those values greater than, or equal to .9 recognised as good fit (Byrne, 2001; Hair et al., 2006; Tabachnick & Fidell, 2007).
3. AGFI (Adjusted Goodness-of-Fit Index) is, in the context of this study, adopted in addition to GFI. Notably, the main difference between AGFI and GFI is the fact that the latter, in the specific model, adjusts in line with the degrees of freedom (Byrne, 2001: 82). Markedly, AGFI values spanning 0-1, with values equal to or greater than .9, are recognised as being a good fit (Byrne, 2001; Hair et al., 2006; Tabachnick & Fidell, 2007).
4. As has been noted by different scholars (Byrne, 2001; Hair et al., 2006), consideration needs to be made of RMSEA (Root Mean Square Error of Approximation), which considers "the error of approximation in the population, and asks the question: how well would the model, with unknown

but optimally chosen parameter values, fit the population covariance matrix if it were available?" (Browne & Cudeck, 1993: 137-138, cited in Byrne, 2001: 84). RMSEA shows the degree of fit between a model and a population (Hair et al., 2006: 748). Furthermore, RMSEA communicates the fit per degree of freedom, and is known to be sensitive to parameters applicable (MacCallum, Browne & Sugawara, 1996). Markedly, RMSEA with values of less than .05 showing a good fit and values ranging .05-.08 are considered acceptable, whilst values of more than .08 are recognised as being poor, and therefore showing an unacceptable fit (Byrne, 2001; Hair et al., 2006; Tabachnick & Fidell, 2007).

Second, it is acknowledged that incremental fit indices are utilised in terms of "assessing how well a specified model fits relative to some alternative baseline model" (Hair et al., 2006: 749). Owing to the fact that the absolute fit indices are unable to draw a comparison between frameworks to a particular null model 3 (i.e. unlike incremental fit indices), incremental fit indices have been utilised by this research, as well as absolute fit indices. More specifically, this study has centred on a number of different incremental fit indices, namely Normed Fit Index (NFI), which draws a comparison between nested frameworks to put it another way, NFI draws a comparison between the framework's $\chi 2$ value of the model with the $\chi 2$ value of the independence model (Tabachnick & Fidell, 2007: 716). It is known that the values of NFI range from 0-1, with values greater than or equal to .9 regarded as being a sound fit (Byrne, 2001; Hair et al., 2006; Tabachnick & Fidell, 2007).

Owing to the fact that the NFI index is unable to control for various degrees of freedom, and underestimates the fit when the sample utilised is small (Byrne, 2001), it is held that the CFI (Comparative Fit Index) may prove to be a better version of the NFI index. The values of the CFI span 0-1 with values greater than or equal to .9 are acknowledged as being a good fit (Byrne, 2001; Hair et al., 2006; Tabachnick & Fidell, 2007). Lastly, the TLI (Tucker-Lewis Index), also referred to as the Non Normed Fit Index (NNFI), draws a contrast between the model's $\chi 2$ value with that of the independence model, and takes into account degrees of freedom for both frameworks (Bentler, 1990), as is the case in the context of this study. Notably, TLI index values span 0-1, with values greater than or equal to .9 recognised as good fit (Byrne, 2001; Hair et al., 2006; Tabachnick & Fidell, 2007).

Third, wherever applicable, this study utilises parsimony fit indices, especially normed chi-square $\chi 2/df$, in order to determine which of the frameworks of those competing is considered the best (Hair et al., 2006). Notably, $\chi 2/df$ ratios on the order 3:1 or less are acceptable (Hair et al., 2006: 748). Goodness-of-fit criteria are summarised in Table 3.4 below.

Table 3.4: Goodness-of-Fit Criteria Adopted in the Study

Fit Index	**Recommended Value (Hair, 2006)**
x 2	Non-significant at p <0.05
Degrees of Freedom (DF)	n/a
x 2 /df	<5 preferable <3
Goodness-of-Fit Index (GFI)	>0.90
Adjusted Goodness-of-fit index (AGFI)	>0.80
Comparative Fit Index (CFI)	>0.90
Root Mean Square Residuals (RMSR)	<0.10
Root Mean Square Error of Approximation (RMSEA)	<0.08
Normed Fit Index (NFI)	>0.90
Parsimony Normed Fit Index (PNFI)	>0.60

Chapter 4 of the study provides an in-depth insight into the findings of both the structural and measurement frameworks. The chapter considers the ways in which the analysis results in added value in terms of examining the study framework regarding the hypotheses' rejection/acceptance of the use of SEM (Structural Equation Modelling), whereas another analysis used in Chapter 5 is utilised in terms of qualitative analysis used to mark participants' SA performance using the quantitative instruments designed based on SEM findings.

3.2.4.2 Lab experiment data analysis techniques (T-Test & ANOVA)

This study consisted of two stages, as explained above. In the first stages, an electronic survey was distributed to a group of cyber security experts asking about Active Situational Awareness and SA agility and quality. The first stage data were then analysed by conducting a SEM analysis that we covered earlier. The result of this analysis was used in the second stage, where the artefact (Data capturing script: appendix 3) had been designed to capture expert SA while applying the Active SA model in the testing environment. Also, the first stage data informed the second stage in building the Behavioural Anchor rating scale and the SA assessment metrics that could capture and assess participants' SA performance. Data collected from this stage were then analysed using an independent sample t-test and ANOVA to identify whether there were significance differences between Passive SA and Active SA. In another words, finding any significant differences between winning attitudes introduced by ASAM and preventive attitudes used currently by cyber defence personnel. Finally, data analysis was conducted in order to study the effect of participants' background and deception and blue team utilisation in enhancing cyber SA. Chapter 5 of this study shows the results of this stage of the analysis.

3.2.5 Scenario Development

The use of the 'scenario' concept is widely used in different areas, such as military, the theatre and software development (Pesonen, 2000). Bartusik & Cabala (1997) describe a 'scenario' as "[o]ne possible picture of future conditions of the object and its environment; above mentioned conditions are described by characteristics of the results of given sequences of events (situations) and factors which

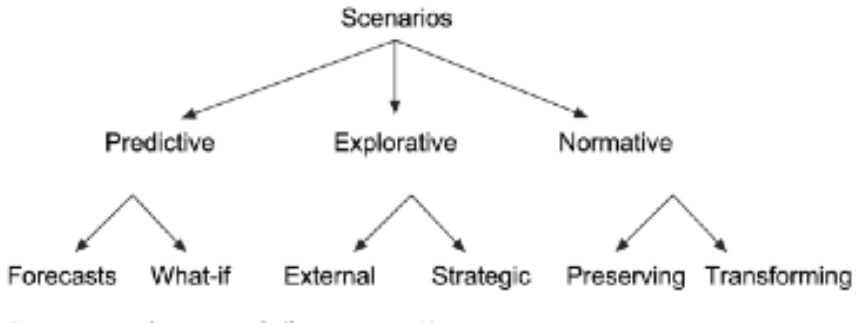
disturb the natural run (evolution) of these sequences". Von Reibnitz (1991) describes a scenario as a description of a future situation and a description of the way that leads to it. Borjeson et al. (2007) created a scenario typology, as shown in Figure 3.6 below. This typology describes the possible future as a result of a scenario. "Predictive scenarios answer the question: 'what will happen?' Exploratory scenarios answer: 'what can happen?' Normative scenarios answer: 'How can a specific target be reached?'" (Borjeson et al., 2007). Therefore, the scenario that will be explored as part of this research concerns the future of the situation that occurs in the present, through playing a cyber game that reconstructs well-known cyber attacks. The main aim of the scenario is to allow the researcher to measure the effectiveness, efficacy and efficiency of Active intelligence in enhancing cyber situational awareness.

The Futures Group (1994) has proposed sets of processes for developing a scenario. These steps can be summarised as follows.

- Define the scenario space or domain.
- Define key measurements and events.
- Documentation.

This research has followed these steps and developed the required scenario, which will be discussed in the section below. The scenario will be designed to allow attacks against the system and breach of network confidentiality. In addition, it will ensure that attacks against the system's integrity and network availability are also included (Tracy, 2009).

Figure 3.3: Scenarios Topology, adopted from Borjeson et al. (2007)



3.2.5.1 The scenario

The scenario selected by the research revolves around the Abu Dhabi Securities Exchange (ADX). The ADX is a leading stock exchange market in the UAE and their mission is to "lead the development of the capital market in UAE through well-regulated marketplace in a lawful environment that ensures integrity, transparency and disclosure". The ADX offers many online services to its customers, including online trading, market news and investor portals, amongst others. In addition, the ADX has provided services to brokers who use the ADX infrastructure to buy and sell stocks in real-time.

Recently, the UAE suffered from political tensions between some external political parties, which did not like the UAE's support for people demanding their freedoms and getting rid of those who used religion to control the people and the country. The UAE stood strongly against those parties by utilising the media and attempting diplomatic solutions; however, a new wave of failed cyber attacks hit UAE cyber resources, but no damage has been reported yet. As a result, the Dubai stock market and ADX agreed to collaborate on and share intelligence about the cyber attacks, and, based on that agreement, each party agreed to report any cyber incident instantly through a common and accessible intelligence reporting system.

3.2.5.2 Building the scenario

In order to build the scenario, there is a need to specify a set of criteria to validate it against. The criteria will mostly be modelled against the five characters as noted by (MNE7 Campaign Lexicon, 2013) which are: Contested, Congested, Cluttered, Connected and Constrained.

Character	Across all Domains	Research Domain
Contested	The ability to access, manoeuvre and influence will be fought for.	Access to the ADX is controlled at different layers according to service and privilege.
Congested	People will be unavoidably drawn into urban areas, the littoral and lower airspace.	For the ADX relates to the congestion of data/traffic and is critical due to the time sensitive nature of the information and market data. Delays could have a detrimental effect on the reputation and usefulness of the data provided.
Cluttered	A mass of ambiguous targets challenge the ability to understand and discriminate.	Due to the multi-tier nature of ADX, it can become difficult to distinguish between investors, brokers, employees and casual (front-end) users.
Connected	All activity, including that of adversaries, will rely on inter-connected networks.	Services provided by the ADX are not limited by geography or any other category.
Constrained	Legal and social norms will place constraints on the conduct of operations.	Finance has an added complication in which there are fine-lines and compliance issues that might not be immediately obvious to the untrained individuals.

Table 3.5: The Criteria of Scenario Development (Source: Author)

Providing further background to the criteria above, it is important to note the following.

Contested: Regarding the layering of access to the ADX, the various levels would be the front-end, which would provide website and emailing facilities. This is for the casual reader or individual requiring more information via email communication. Secondly, there would be a service level that provides registered investors and organisations such as auditors with access to various market data and trading services. Lastly, there would also be the internal level, which is restricted to employees and the management of the ADX, such as reconciliation and end of day processes.

Congested: For the ADX this is quite critical due to the time sensitive nature of the information and market data. Data sources travel from various systems and throughout the various "offices" of the ADX, such as front office, middle office and back office operations. In a given trading day, especially during peak trading hours, the volumes of messages that would pass through the ADX would be very large.

Cluttered: Due to the multi-tier nature of ADX it can become difficult to distinguish between investors, brokers, employees and casual (front-end) users. The nature of finance also makes it difficult to distinguish between the various authorised/favourable users, malicious hackers (technical perspective), money-launderers (financial-perspective) and insider-traders (both) for example.

Connected: Services provided by the ADX are not limited by geography or any other category. Foreign banks or non-domicile investors are able to use the information offered. In addition, orders can be routed by various third-party providers and brokers, which can obfuscate the source of the data.

Constrained: Finance has an added complication in that there are fine lines and compliance issues that might not be immediately obvious to the untrained individuals, as well as legal requirements such as Know Your Client (KYC) checks, Politically Exposed Person (PEP), insider trading (providing important information that will unfairly bias a market) and bribery tactics (again a fine line between gifting and bribing).

3.2.5.3 Validating the scenario

The proposed scenarios would need to address each point, which in turn would lead to a validated approach. Key items of the mission and objects are noted below.

1. Ensure ADX remains up and running.
2. Ensure ADX is secure from cyber attacks.
3. Ensure partners and investors are able to access the services during critical trading periods.
4. Ensure Auditing companies are able to access the services securely.
5. Ensure critical news portal service is accurate and valid.

3.2.5.4 The mission and objectives

The experiment mission as a cyber commander is to ensure that the ADX system stays up and running, secure from cyber attacks, and able to handle the fact that the ADX has databases accessed by many partners remotely, where partners' IPs are dynamic. The availability of the system is crucial during the trading period, and its integrity is important as well.

An additional complication is that the ADX allows auditing companies to access their networks using a VPN service, whereby the username and password are the only authentication methods used for this

service. Auditing usually starts after trading period, where all data will be audited during that time. Finally, the ADX portal is a critical news portal for traders, as the ADX provides investors with the latest news about registered companies.

The objective of this scenario in this research is to allow participants to employ an active C2 new approach towards cyber security discussed in this research, as well as identifying the significance of situational awareness and showing how active intelligence can help in enhancing organisations' cyber situational awareness quality and agility. Moreover, the scenarios have been designed with the aim of establishing whether participants can detect cyber attacks and are able to predict the cyber situations throughout the scenario.

Last of all, the participants are required to watch the testing environment and make sure of the availability, integrity and confidentiality of its data. Also, participants must utilise the new features added to defend and respond to cyber attacks using the offensive methods. As described, this experiment is about testing the new, winning attitude instead of the current, defensive approach. More detail can be found in appendix 3.

3.2.6 Data Gathering Instruments Adopted in this Thesis

A critical process of a research project, as stated by Krathwohl (1997), is collecting data through inquiry methods that are guided by the purpose of the research and which are influenced by the investigation of the researchers. The instruments for data gathering (methods of inquiry) of the current research were accordingly chosen on the basis of its research goals and philosophy. This research mainly uses the survey method, as it was considered to have greater advantages compared to other instruments (Krathwohl, 1997; Galliers, 1992). The first survey was circulated as an electronic survey amongst cyber security experts to establish an early theoretical model that could be validated. This survey had closed questions, and was entirely quantitative in nature. Serious gaming environment was designed and developed so the causal model of active SA can be validated in practice. A semi-structured survey that had open-ended questions, and was followed up by a qualitative approach (4 main SA questions), was the second instrument of data collection, used during the lab experiment, which was then used to measure participants' SA using the quantitative instruments developed during this study. This section further elaborates on these instruments of data collection.

3.2.6.1 Stage one: data instruments

Section 3.1 of this chapter discussed how important it is to utilise the collection of knowledge from existing literature, and argued that the researcher needs to learn from the pioneering works of the earlier research. Chapter 2 focused purely on building the theoretical framework of active SA on previous existing literature and critically designing the conceptual hypothesised active SA model. Section 2.5 critically analysed the current literature and provided the theoretical framework of active SA. The variables extracted there were grouped into tables 6 and 7. Therefore, the following statements have been designed based on information derived from a critical review of literature and the initial online survey to shape the hypothesised model of this research study. The data derived from this survey

are then analysed using SEM, to test and estimate the causal relations of the active SA model. Check Chapter 2 and Appendix one for more detail.

Table 3.6 shows the survey code sheets and how they are related to literature.

Table 3.6: Initial Survey Statement (more detail in Appendix 1)

Construct	***Items***	***Variable Description***	***Question***	***Source (Ref)***
Quality and Agility (QA)	ES1	Timeliness	Situational Awareness is agile when Situational Awareness achieved in a timely manner.	Albert & Hayes, 2006: 125; Endsley, 2000
	ES2	Responsiveness	Situational Awareness is agile when an organisation has the capability to act within a window of opportunity during the cyber incident.	Albert & Hayes, 2006: 125
	ES3	Adaptability	Situational Awareness is agile when an organisation can adapt to changes quickly.	Albert & Hayes, 2006: 125
	ES4	Quality Accuracy	High quality Situational Awareness relies on accurate information.	Albert & Hayes, 2006: 125; Lehr & Pupillo, 2009
	ES5	Quality Reliability	The reliability of the source is needed to produce high quality Situational Awareness.	GAO, 2000
	ES7	Quality Timeliness	High quality information provided in timely manner helps to enhance cyber Situational Awareness.	Albert & Hayes 2006: 125
Intelligence				
1- Passive Intelligence (PI)	in1	Intelligence Timeliness	A good intelligence is one that has been provided in a timely manner and is useful for an organisation to enhance its cyber Situational Awareness.	Peterson, 2013
	in2	Enemy IP	IP (Internet Protocol) identification is a key factor to build cyber Situational Awareness.	Gordon, 2005
	in3	Enemy Motive	Identifying the motive behind a cyber incident is vital for an organisation to build a strong Cyber Situational Awareness.	Varon, 2002; GAO, 2000
	in4	Passive Intelligence Gathering Capability	Intelligence gathering capabilities during a cyber incident is important for an organisation to handle enemy attacks.	Huey & Rosenberg, 2004: 598; Beaver et al., 2011
	in5	Intelligence Sharing	Sharing intelligence resources and capabilities are required to build strong and reliable cyber Situational Awareness.	House.gov, 2013: 3
	in6	Intelligence Collaboration	Cyber collaboration is important to build strong and reliable cyber Situational Awareness.	Kaser, 2012: 3
	in7	Interaction Capability	The more interaction an organisation has with the enemy, the more knowledge an organisation can gather about the enemy.	Huey & Rosenberg, 2004

2- Active Intelligence (AI)	in8	Enemy Capabilities	Information about the enemy's capabilities (operating system, services running, tools used) enables a defending organisation to evaluate the threat possibilities, which helps to enhance cyber Situational Awareness.	Holdaway, 2001
	in9	Enemy Weaknesses	Identifying enemy weaknesses during a cyber incident helps an organisation to enhance Situational Awareness based on enemy vulnerabilities.	Holdaway, 2001
	in10	Intelligence Accuracy	Intelligence accuracy in cyberspace is vital in order to enhance cyber Situational Awareness.	Albert & Hayes, 2006: 125
	in11	Intelligence Completeness	Completeness of cyber intelligence is required to enhance an organisation's Situational Awareness	Albert & Hayes, 2006: 125
	in12	Information Gathering	Within an offensive approach, a deceptive capability (active intelligence gathering) provides superior information that enhances cyber Situational Awareness	Chen, 2010
	in13	Destroy	Information about how to destroy an enemy in cyber space helps in enhancing the defending organisation's Situational Awareness	Holdaway, 2001; Gary, 2011
	in14	Active Intelligence Gathering Capability	Active Situational Awareness through active intelligence gathering is required for future cyber security.	Chen, 2010; Varon, 2002

3- Intelligence Gathering	in15	Resources Availability	Resource availability helps to enhance cyber Situational Awareness.	Theohary & Collins, 2011
	in16	Non Cyber intelligence	Combining other non-cyber related sources of intelligence helps to enhance an organisation's cyber Situational Awareness.	Albert & Hayes, 2006: 125
	in17	Enemy Geo Location	The attacker's geographical location helps an organisation to enhance cyber Situational Awareness.	Gordon, 2005
	in18	Enemy Attack Variation	The defending organisation with deception capabilities can enhance cyber Situational Awareness by deceiving an enemy to identify all possible enemy attack variations.	Chen, Tan, Xing, Wang & Fu, 2010: 1739
	in19	Enemy Attack Consistency	The defending organisation with deception capabilities can enhance cyber Situational Awareness by deceiving an enemy to identify enemy attack consistency.	GAO, 2000
	in20	Granular Level of Threat Detail	A granular level of threat detail helps to enhance an organisation's defence.	Albert & Hayes, 2006: 125
	in21	Enemy Possible Attack	Within an offensive approach, information about a possible attack which has an impact on enemy resources helps the defending organisation to enhance its Situational Awareness.	Salerno & Tadda, 2009: 1
	in22	Enemy Attack Timing	The defending organisation with deception capabilities can enhance cyber Situational Awareness by deceiving an enemy and so identify enemy attack timing.	GAO, 2000

Situational Awareness (SA)	S1	Perception Correctness	Perceiving incorrect data leads to poor cyber Situational Awareness, so training techniques and procedures employed by the defending organisation help to avoid such an issue.	Albert & Hayes, 2006: 125
	S2	Perception Completeness	Poor cyber Situational Awareness results from perceiving incomplete data, so training techniques and procedures employed by the defending organisation help to avoid such an issue.	Albert & Hayes, 2006: 125
	S3	Previous knowledge	An organisation that has rich and accessible previous information (such as vendor reports, previous cyber incidents, risk assessment reports, cert reports etc.) allows an organisation to build strong cyber Situational Awareness.	Nonaka & Nishiguchi, 2001
	S4	Skill	Comprehension of the cyber incident situation is gained when an organisation relies on skilful and experienced employees.	Nonaka & Nishiguchi, 2001
	S5	Analysis Capability	Cyber threat analysis is key to the comprehension of the cyber incident	Endsley, 2000
	S6	Confidence	Cyber Situational Awareness requires both willingness and trust to use cyber intelligence.	Tadda, 2008; Albert et al., 2006
	S7	Projection (intent)	Estimating the enemy's intent towards the defending organisation's assets can enhance Situational Awareness.	Salerno & Tadda, 2009: 1

3.2.6.2 Stage two: research experiment environment development and data instruments

This section discusses the second stage methodology adopted in this research. SEM results in this research are used to develop the serious gaming environment, the active SA behavioural anchor rating scale and the SA assessment metrics. The serious gaming environment is an environment that allows researchers to assess participants' SA in regard to cyber incidents. In the current research, the environment was developed through several stages, as described in this section. The SEM result also informed the development of SA assessment scales, where factor loading was used to define the weight of each variable in the active SA model, and the factor coefficients of determination and causal relations were used to determine how much each factor contributes to the active SA model. This section will provide more insight into the stage two experiment and instruments.

Problem Identification and Motivation: Malicious attacks on computer network systems pose immense threats to the computer networks of any organisation. Therefore, it is necessary to ensure that extraordinary measures be deployed to ensure that these risks are properly mitigated. However, before designing the measures, it is important that all situations posing threats to the computer network systems of an organisation are determined. Only then can benchmarks be established, statistics generated and success rates determined.

Situational awareness (SA) is crucial in aiding organisations to come up with the awareness of various threats and scenarios, besides conducting an exclusive estimation of the various implications of imminent attacks. The use of SA also helps to create heightened awareness and understanding of all situations that might be risky to the security of any information system.

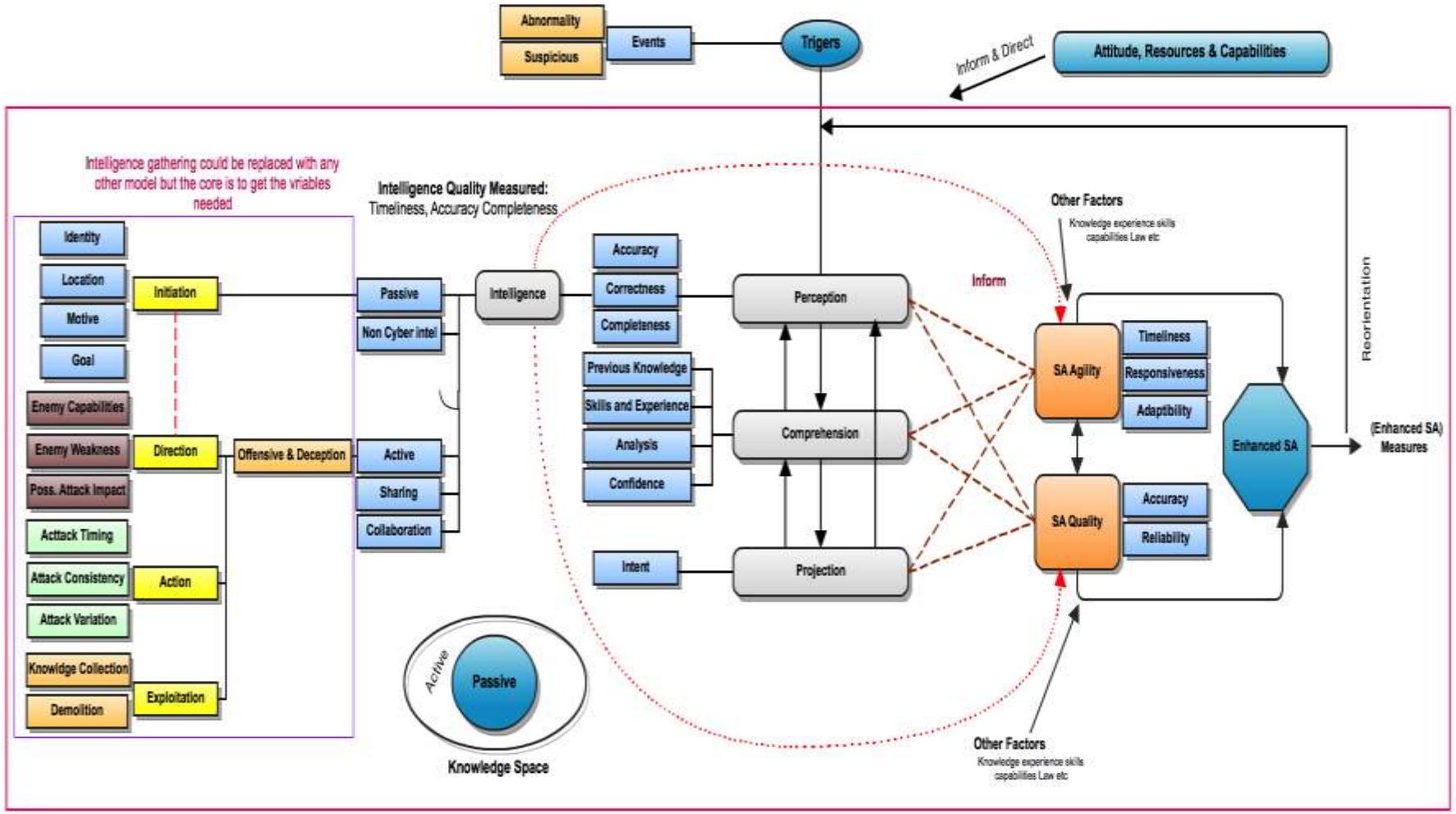
Current cyber situational awareness models were built with passive defence in mind, and that simply cannot provide the necessary capabilities to deter advanced cyber threats. Chapter 2 discussed some of the issues related to cyber security and cyber SA and its limitations within current SA model, and the problem is that most current cyber security SA models are passive character and not aligned correctly with doctrine, which makes them vulnerable to modern evolving cyber attacks. In a world of rapid change and increased resources, it is imperative that Active SA is employed to stay ahead of the game and adapt ahead of the threats, whilst still taking advantage of past knowledge. Static and passive systems are incredibly slow to adapt, and, in the case of cyber war, which is a war of information, the side that has more information simply wins. This is the reason why active defence (offensive approach), employed with a winning attitude, should be in place. A situational awareness model should be designed with a winning attitude that aligns correctly with doctrine which provides superior quality information in a timely manner that eventually provides an organisation with the agility to respond to an attack. This preventive attitude is discussed in Chapter 2 – as the name suggests, it prevents defenders from being able to predict future events/targets of cyber attacks. Therefore, the sort of winning attitude discussed in Chapter 2 is the most suitable option for cyber security, and helps the defender gain advantages over attackers.

Sun Tzu discussed the importance of having good intelligence about the enemy to win a war, and he went further, by making intelligence the central point in defeating an enemy. Endsley (2000) argues that, from an intuitive point of view, SA is all about "knowing what is going on", and her research shows the importance of information flaws so that an organisation can get a better understanding of the environment it deals with. Tadda's (2008) SA model describes the importance of cyber sensors in the network in order to activate SA. This ensures that information is captured locally in order to determine the situation in the network environment. Using such technology would help to solve the complexity of the digital world and identify the offender. Palermo & Kocsis (2005) argue that local sensors such as IDS, firewalls and system logs are crucial in any cyber defence, as these tools shape importance sources in investigating cyber attacks, and also help in identifying the IPs and location of the offenders, and even sometimes help in understanding their method of attacks (Jone et al., 2006; Da-Yu Kao & Shiuh-Jeng Wang, 2009).

In ethical hacking, hackers usually start penetrating after gathering some intelligence about the target. The main intelligence they pursue is the target's IP and ports (Gordon, 2005). In this thesis, active intelligence is about collecting intelligence about an enemy by using an aggressive method. The local sensor would help in capturing the suspect IP (Jones et al., 2006) that will allow the defending organisation to start attacking and gathering intelligence in the same way that hackers do.

Albert & Hayes (2006) argue that agility and quality of information should be considered when building cyber SA, and that intelligence is the centre point of doing that. Accuracy, timeliness, responsiveness and reliability of intelligence are all important if SA is to be achieved in a quality and agile manner. From the above discussion, and from the previous literature discussed in Chapter 2, a theoretical model was developed (Figure 3.4) and designed to align with military doctrine in order to overcome the limitations of the Cyber SA model by introducing a winning attitude that would use offensive measures to gather intelligence from the enemy's domain. This model answers all questions concerning the design science early stages. It also provides guidance on building research instruments

Figure 3.4: Active Situational Awareness Hypothesised Theoretical Model (Source: Author)



Experiment Aim &Objective: The aim of this experiment is to test the usefulness of the active SA in building cyber situational awareness through the utilisation of an active offensive approach. The main objectives are as follows.

1. Capture participants' SA to measure SA effectiveness and efficacy.
2. Capture participants' decisions and actions.
3. Measure participants' SA quality and agility.

Hypothesis: Active Intelligence Gathering using *Offensive Hacking* techniques helps to *Enhance Cyber Situational Awareness* through enhancing an organisation's *Agility* and *Quality* in dealing with cyber incidents.

3.2.6.3 Design and development of research serious gaming environment

This part of this section will cover all the aspects of developing the serious gaming environment that meets this research requirement. The theory of active SA and SEM structural model informed directly the development of this research serious gaming environment through providing main factors and components that required for active SA environment. Also the scenario of this research covered earlier in section 3.2.5 informed the development as it identified the main objective of the serious gaming environment. This part of this section will provide more insight into the serious gaming environment infrastructure and components.

System Requirements: The required system can be described as an intelligence gathering system, using multiple sources of intelligence to deliver high quality and agile situational awareness to cyber commanders, as recommended by Alberts (2002). This system relies on three different intelligence sources:

1. Active intelligence gathering using offensive hacking and deception techniques, providing cyber commanders with intelligence from enemy domain (Cahanin, 2011; Nakashima, 2010; Thomas, 2009).

2. Passive intelligence based on local security controls (Li et al., 2009) and sensors providing cyber commanders with local captured intelligence.

3. Intelligence sharing and collaboration across partners (Kaser, 2012: 3) that allows cyber commanders to have more capability to handle cyber conflict.

The system should provide varieties of monitoring solutions that allow operators to monitor the entire organisational network's assets with sufficient visualisation tools, and it should be designed to enhance cyber commanders' situational awareness by utilising multiple sources of intelligence in a clear and consistent manner. It is hypothesised that the active components in this system will give commanders

competitive advantages over their opponents, where intelligence can be taken from the enemy domain using active offensive techniques.

Based on what has been discussed in this chapter, in order to test ASAM, the following requirements should be considered while developing the testing environment:

- A computer network environment that reflects the real, physical world with real assets.
- Real network traffic with real noise.
- Network and security alerts dashboard.
- Network and security monitoring dashboards.
- Central point of control of the entire environment.
- Intelligence reporting system to deliver intelligence across participants.
- Sharing and collaboration regarding cyber security incidents across different stakeholders.
- Offensive capabilities with advance hacking tools and deception capabilities.
- Network and system control capabilities.
- Capabilities to freeze and stop the entire network environment without altering its normal execution.
- Red team (enemy) to attack the designed system from the Internet.
- An instrument to capture expert participation and SA.

In order to achieve the above, the system requires highly sophisticated technologies that can provide real-time awareness of a particular cyber incident. This can be achieved by integrating different types of technologies that offer real-time network monitoring and visualisation services.

The use of an intelligence reporting platform is crucial for cyber commanders because such a platform would allow the intelligence feeds to be delivered in a timely manner. Therefore, due to these complex requirements, this researcher decided to include the following characteristics into the system design.

1- Intelligence reporting system:
This system allows intelligence to flow across participants in timely manner, with functionality to receive, store and send intelligence within a central database. The system would help cyber commanders to have access to important intelligence so better situational awareness can be achieved. Speed and efficiency would be paramount, especially over time when the data consumed and processed would greatly increase and the system would still continue to behave consistently as per the user's expectations.

2- Blue Team:
A blue team enabled cyber system gives the cyber commander the ability to act in an enemy network. Intelligence from such a source would allow an organisation to enhance its defence, and be able to tackle a cyber incident in a more sufficient way, as well as to be able to build up an enemy's profile.

a. Passive security controls

IDS, firewalls and other monitoring technologies are important sources for spotting suspicious activities that cyber commanders can rely on. In this system, different tools are integrated to provide high visualisation results of the network activities.

b. Intelligence sharing and collaboration:

Partners can provide high value intelligence that organisations can rely on in improving cyber capabilities. This system provides such services and makes them available to cyber commanders so that better resource utilisation and defence can be achieved.

c. Deception center (cloned controlled DMZ)

This service is available to cyber commanders to utilise during cyber incidents. This would allow intelligence to be gathered as enemy activities are monitored and controlled.

3- Red Team:

A red team in this experiment will act as an enemy. The main objective of this red team is to penetrate the testing environment and challenge commanders and their security controls.

3.2.6.4 Operation of serious gaming environment

1- Pre-cyber conflict:

The system operates with a winning attitude in mind. A cyber commander of a cyber operation is responsible for providing clear mission objectives and focusing the people in charge so that high quality and agile SA can be achieved (Sawyer, 1994). Blue team is in charge of utilising all possible skills and deploying new sensors or monitoring pre-existing sensors to gather intelligence from the enemy domain, and providing this intelligence to cyber commanders. Cyber commanders may direct blue team in their mission so the required intelligence can be provided. In case of enabling deception services, blue team should be in charge of monitoring enemy activities and providing cyber commanders with the latest intelligence report. On the other hand, operators in this system are in charge of keeping the organisation's network system safe and up and running through the utilisation of the local security sensors. The available resources in this system are capable of keeping the cyber commanders updated with the status of the system's health and performance. Also, they can provide the necessary intelligence in case of a cyber breach. Intelligence provided by partners whom agreed to share cyber breach intelligence is vital to allow cyber commanders to build strong situational awareness, and so such intelligence should be examined and assisted by cyber commanders, who may ask members of the team to validate it. This intelligence could direct cyber commanders to effect changes in the operation's plan or even help in updating the organisation's security defence. Deception services can only be activated by a cyber commander who is in charge and who can give operators the order to channel suspicious traffic towards the deception centre. The blue team is responsible for monitoring the deception service, and provides the intelligence about enemy movements to the cyber

commanders. In this exercise, one person will fulfil the role of providing the offensive capabilities service to the cyber commanders (participants). Red team, in this experiment, is in charge of penetrating and challenging the participants' network, and will be handled by a different person.

2- Cyber conflict:

During a cyber conflict, the active SA system would provide superior intelligence at the operational and tactical level, as recommended by Parks & Duggan (2001) and Sawyer (1994). The system would help cyber commanders to enhance intelligence gathering, and hence inform the commanders' decision-making process. Target acquisition in this system means having an ear on the enemy domain, where blue team uses it to extract intelligence and deliver it to the cyber commanders to exploit. Also, the system would direct cyber commanders in setting priority, and influence commanders in giving orders and direction during cyber conflicts. With respect to the control group, the serious gaming environment will provide only passive components. The cyber commanders in this case will try to defend the organisation assets using passive security controls only. The blue team (offensive capabilities) and deception service will be disabled.

3.2.6.5 Employment of serious gaming environment

In order to get the full benefits from the system, the commander's structure needs to be defined and authorisation distributed based on needs (Albert & Hayes, 2006). Also, the Active SA system requires a winning attitude to be adapted so the cyber team can utilise all available resources when needed. In this system we have three main players, as described below.

Cyber Commanders: in charge of monitoring network assets and the intelligence reporting system. Also in charge of leading both the blue team and cyber operators. The commanders (participants) in this experiment act as incident handlers, vulnerabilities and threats analysts and decision makers. Therefore, participants are going to act as a cyber commanders and cyber operators.

Blue Team: in charge of monitoring organisation networks, and use offensive hacking and deception techniques to gather more intelligence from enemy domains. Obey the commander's instructions and update him with real-time intelligence feeds.

Cyber Operators: in charge of monitoring the organisation network and trying to spot any suspicious activities by using the provided monitoring and visualisation technology. Obey the cyber commander's instructions and do the required changes in the network environment. Therefore, cyber commanders should give other cyber staff some responsibility and authorisation, especially the blue team, where fast decisions should be made when it comes to intelligence gathering from the enemy domain.

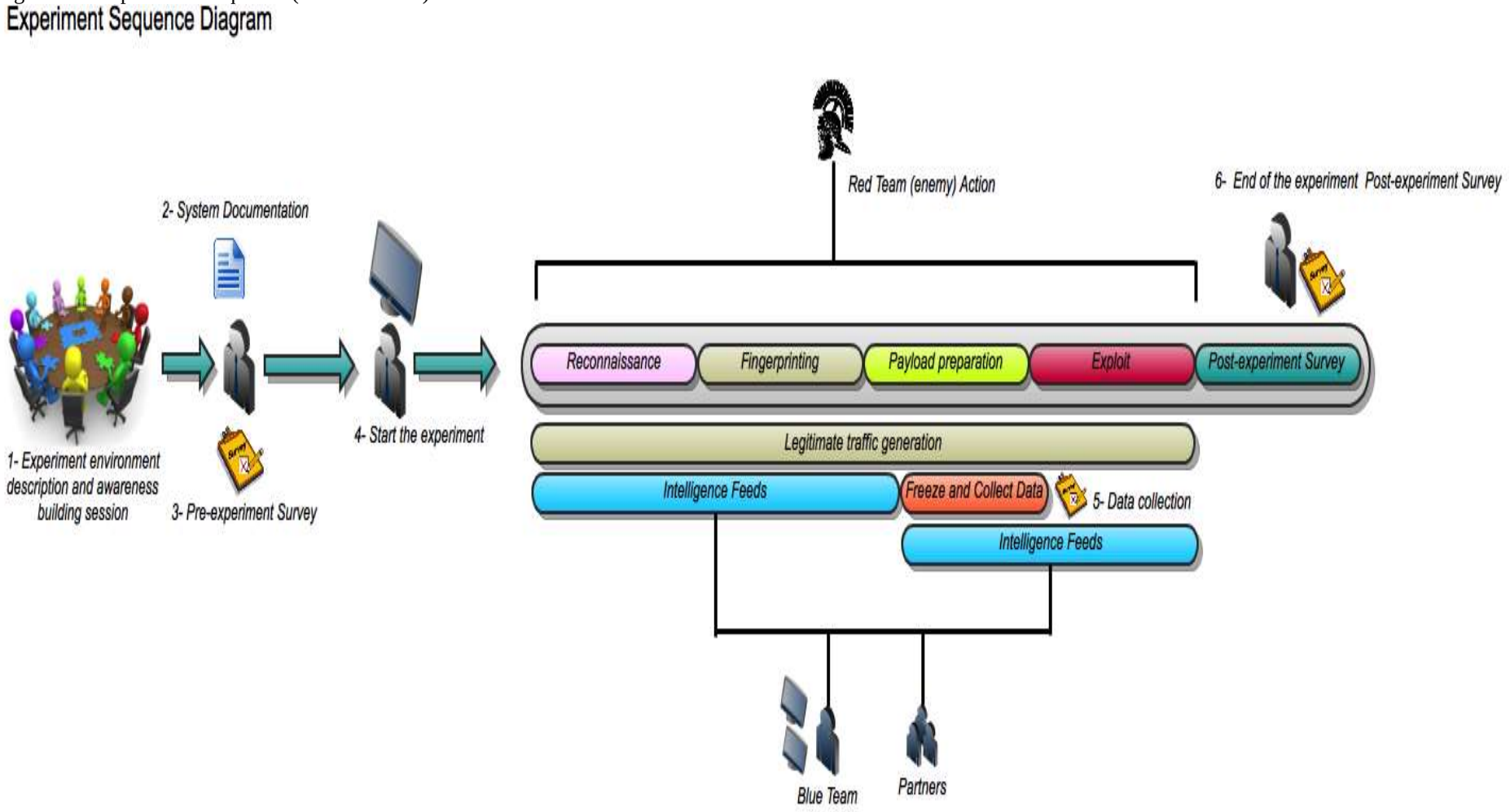
3.2.6.6 System coverage

The system will cover organisation networks assets by utilising local sensors. Also, the system would allow an organisation to act in the enemy domain by utilisation of remote sensors used by blue team. Partner's intelligence is covered in this system as a subscriber can enjoy the benefits of intelligence feeds and support from other cyber operation centres.

3.2.6.7 Experiment sequence

The experiment has been designed based on the requirements discussed earlier. Most of its sequence derived from or rely on existing literature in the area of ethical hacking, networking, command and control, security and situational awareness. The scenario employed in this thesis was designed based on principles employed by military that cover concept of use, concept of employment and concept of operation. The red team in this research is the enemy that will be launching attacks using kill chains, as described by Kjaerland (2005). It worth's to note that different scholars have different labelling for the kill chain, however the process is still the same. The attacks in this experiment are categorised as following: attacks against system and network confidentiality; attacks against system integrity; attacks against system and network availability (Tracy, 2009). The research scenario development relied on these attacks to come up with a scenario that reflects the real world situation, which will be discussed later in this chapter. Sommers et al. (2004) argue that "the ability to generate repeatable, realistic network traffic is critical in both simulation and testbed environments" in order to make the environment behave like or reflect the real situation. In this research, traffic generation is real traffic coming from clients both in and outside the testing network, accessing available resources. Figure 3.5 below shows the sequence of the ASAM experiment that summarises 6 points, starting by providing participants' information about the experiment and clarifying the aims and objectives of this experiment. It then provides more detail about the testing environment by allowing them to read the system specification and documentation. Data collection for each session is divided into 3 stages. It starts with pre-survey, collecting demographic data of participants. The second stage is more concerned about participant SA and intelligence. Finally, at the end of the experiment, participants are asked some questions related to SA and their point of view regarding the aSA approach to cyber security. In the instrument section that follows, more detail will be provided.

Figure 3.5: Experiment Sequence (source Author):

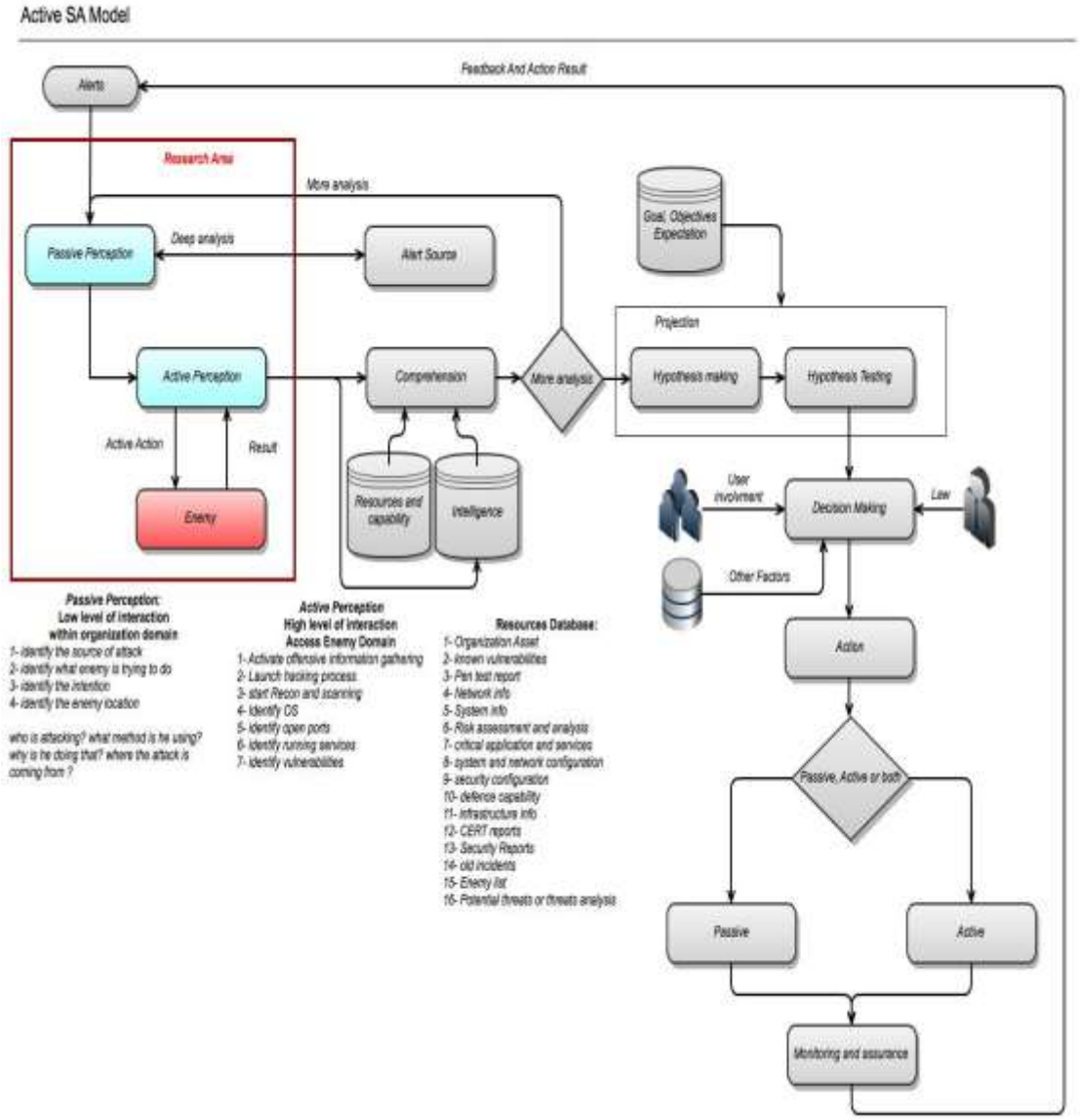


3.2.6.8 Development of the experimental testing environment and piloting

By following Peffers and colleagues' (2007) recommendation, the system and the SA assessment framework were developed in accordance with the requirements described in this section. During its development, the researcher managed to expose the system and SA assessment metric to cyber security experts for the purpose of making sure that it reflected real network behaviours and the metric is valid for evaluating cyber SA. Many enhancements were made until the researcher managed to deliver the final product. The system has been piloted, and the researcher made sure that participants could easily understand how to operate it. Moreover, due to SAGAT requirements, Endsley's (1990a), to capture participants' SA, the system includes a feature that allows the researcher to freeze the testing environment and save a copy of its execution without affecting its integrity. Therefore, the proposed system in this research would allow the researcher to put the theoretical model into practice and validate it.

Theory is important for design science (Venkatesh, 2000), as it acts as starting point to understand what artefact is needed. In this research it is clear that the main requirement is to develop an assessment metric that allows to quantify SA and develop a system with an active intelligence features, and which is capable of capturing all the required measurements. The theoretical active SA model inform the development of this testing environment as it is clear main active components should be included in any active SA environment. In order to do so, the process model set out below (Figure 3.6) was developed to the aSA theoretical model (Figure 3.4) in practice. (More details of this model are in Chapter 2).

Figure 3.6: The Process Model of ASAM (Source: Author)



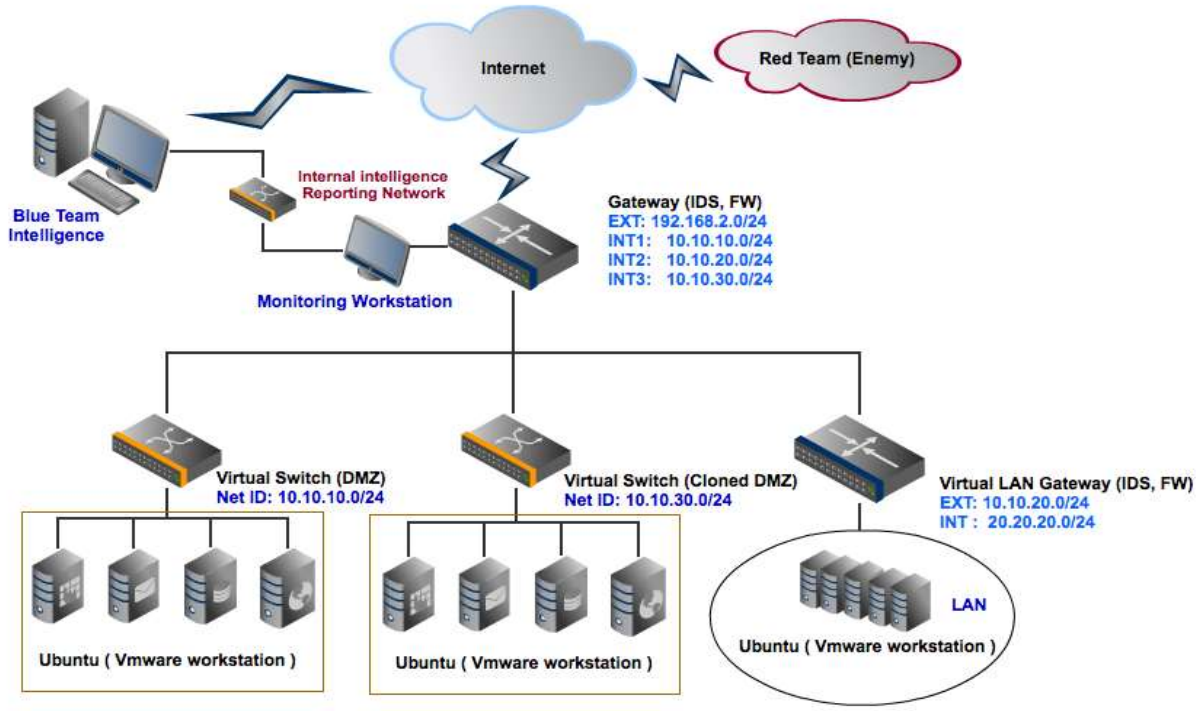
The following section will discuss the serious gaming environment design and development where system components and network typology used for testing active SA approach are described in detail.

a. System infrastructure components: The development of testing environment requires tools and devices similar to those tools used by any organisation complex network. This research thought to build a cost effective serious gaming environment that reflects real organisation network but in virtualised environment which is considered cheap and cost effective technology to mimic a real network assets using few hardwares. Due to the nature of this research, security controls will be included in the environment, such as IDS, network monitoring tools and antivirus. This research considered using commercial-like security controls products that are available for free as open source, where a community of security experts participates in developing such tools. In order to achieve the required features the below components were integrated.

- **Gateway**: Linux based gateway called (Zentyal) used as an internet gateway and client LAN gateway.
- **IDS**: Snort and suricate.
- **IDS Visualization**: Snorby and Squi.
- **Firewall and antivirus**: Zentyal (Linux open source edition).
- **Network Monitoring and Analyser**: Cola Soft (Capsa).
- **Freezing and revert option**: this feature has been added so the entire environment can be controlled. The script has been written using a shell that relies on vmrun package.
- **Kill chains**: used by red team and blue team where each scenario will be played in a fully automated way. However, human involvement is required to execute shell scripts and select the proper attack needed.
- **Virtualization**: Vmware workstation (8&9) and Virtualbox.
- **Vswtiching**: Vmware and other Linux based.
- **OS**: Ubuntu, Windows server 2008, Windows 7 Windows XP, Debian, Fedora and other Linux based OS.
- **Servers**: Windows server 2008, Windows 7, PPTP server and Ubuntu.
- **IDS OS**: Debian.
- **VM OS**: Ubuntu.
- **Clients**: Windows 7, Windows XP and Ubuntu.
- **Red Team**: Windows XP, Backtrack, Ubuntu.
- **Blue Team**: Kali Linux, Backtrack and Ubuntu.
- **Other Tools**: MSQL Client, Browser, Email Client, Shell and Python.
- **Intelligence Reporting System**: (Subscriber System, Provider System, Blue Team intelligence reporting system) system used to distribute or share intelligence with DM. This system has been design using shell script (for more details see appendix 3).

b. Network typology:

Figure 3.7: Serious Gaming Environment Network Typology (Source: Author)



In this research experiment we followed two phases, as described in this chapter, where the first phase was to develop the theoretical model, and to test estimate and causal relations, using SEM, to determine the goodness-of fit, and examine the relationships among multiple independent and dependent constructs. The combined summary of all the results of this phase can be found in Chapter 4, and ultimately the results were used to shape the system design of ASAM. This was done primarily by using the metrics identified, and the system was validated against it throughout all phases of the design.

The second phase was to put the results of SEM into practice, where the researcher captured the experts' view of active intelligence. SAGAT provides an objective measure of SA for knowledge labelling in manned simulations of the task environment, where it directly compares operators' reported SA to reality. SAGAT intervenes in a human-in-the-loop simulation at specific times, and queries the subjects by using a computerised tool for determining their current understanding of the situation at that particular point in time (Endsley, 1990a). Therefore, this research adopted SAGAT to capture participants' results using a semi-structured survey (more details about SAGAT have been discussed earlier in section 3.1.5 and will be discussed further in the section 3.2.6.11).

3.2.6.9 Lab experiment stage two instrument

The participants in the experiment were required to provide some demographic information, such as their name, age, gender, job role, education etc. During the experiment, one of the research groups recorded the participants' activities and captured the timestamp of each event. A different person recoded the time log of the red team. Finally, the participants were required to repeatedly answer the following questions whenever they encountered a suspicious event, which was a non-intrusive SAGAT

techniques, and the questions were used to help identify the perception, comprehension, projection and action/decision of the participant, as described by Endsley (1995) (Appendix 3)

What is going on in the network? What do you see?
What does it mean?
What is your Situational Awareness?
What is your action?

Based on the above questions, the participants' behaviour was estimated using the Behaviourally Anchored Rating Scale (SA BARS) that describes a participant's performance in response to cyber incidents based on ground truth, shown in Table 3.7, below. The experiment kill chains was developed and validated through subject matter experts where group of cyber security experts participated to develop this research kill chain. As discussed earlier, different scholars have different kill chains but in reality it is just a different labelling of the same process.

Table 3.7 Experiment Kill Chains

	Reconnaissance					
Scenario Ref	***Scanning***	***Fingerprinting***	***Payload Prep.***	***Attack Execution***	***Attack Type***	***Exploit***
ASAM01	2 mins.	2 mins.	3 mins.	90 secs.	Denial of service (system level)	Desktop Communication Service
ASAM02	2 mins.	2 mins.	5 mins.	6 mins.	Database brute force and unauthorised access	Windows 2008 SQL server
ASAM03	2 mins.	2 mins.	3 mins.	5 mins.	PPTP VPN brute force	PPTP Server
ASAM04	2 mins.	2 mins.	90 secs.	3 mins.	Escalating privilege attack	Windows Share
ASAM05	2 mins.	2 mins.	90 secs.	1 mins.	Denial of service (system level)	Windows BIOS

3.2.6.10 SA BARS

The researchers at the University of Queensland were among the first to develop a Situational Awareness Behaviour Anchor Rating Scale (SA/BARS), using it to measure the SA performance of the members of Air Services, Australia. This technique involves expert observers rating individuals on the basis of the 28 observable behaviours (Table 3.8) that are indexed to SA processes (Mathews et al., 2000). It uses a 5-point Likert scale, where the performance in terms of specified behaviours is rated as either very poor, poor, borderline, good or very good. One view of the 28-framed SA behaviours suggests that it can also be generalised for other networks.

Table 3.8: SABARS Rating Items (Example. Mathews et al., 2000)

1. Sets appropriate levels of alert.
2. Solicits information from squad leaders.
3. Solicits information from civilians.
4. Solicits information from commanders.
5. Effects coordination with other platoon leaders.
6. Communicates key information to commanders.
7. Communicates key information to squad leaders.
8. Communicates key information to other platoon leaders.
9. Monitors company net.
10. Assesses information received.
11. Asks for pertinent intelligence information.
12. Employs squads tactically to gather needed information.
13. Employs graphic or other control measures for squad execution.
14. Communicates to squads overall situation and commander's intent.
15. Utilises a standard reporting procedure.
16. Identifies critical mission tasks to squad leaders.
17. Ensures avenues of approach are covered.
18. Locates self at vantage point to observe main effort.
19. Deploys troops to maintain platoon communications.
20. Uses assets to effectively assess environment.
21. Performs a leader's recon to assess terrain and situation.
22. Identifies observation points, avenues of approach, key terrain, obstacles, cover and concealment.
23. Assesses key finds and unusual events.
24. Discerns key/critical information from maps, records and supporting site information.
25. Discerns key/critical information from reports received.
26. Projects future possibilities and creates contingency plans.
27. Gathers follow-up information when needed.
28. Overall situation awareness rating.

SABARS was derived from the researched instruments of individual assessment, such as the Comprehensive Assessment of Team Member Effectiveness (CATME), which is founded on the teamwork literature and on the Likert-scale format, with an aim to identify the possible ways to enhance the effectiveness of a team. This instrument forms the basis of one of the SA BARS that assesses five broad areas of team-member contribution, where the people who perform the rating activity are required to make only five decisions about each person they rate (Campbell et al., 1973; Loughry, Ohland & Moore, 2006).

The main advantages of SABARS are that its rating scale uses 'behavioural anchors', it is relatively simple to use and it is unobtrusive. Altogether, the usefulness of SABARS rests on the fact that they facilitate a detailed measurement of the major SA behaviours of an individual, which in turn contributes to strengthening SA management. Since SABARS involves expert observers, the outcomes are expected to be highly reliable, and observer-rating techniques have become more common for their usefulness, such as in facilitating 'on-field' SA assessments by subject matter experts (SMEs), who observe the participants performing tasks under analysis before rating each participant. SABARS' non-obtrusive nature, detailed approach to assessment, ability to measure SA in real time, and high compatibility with the C4i environment (Command, Control, Communication, Computers and Intelligence) are its main advantages (Salmon et al., 2006).

Table 3.9 shows the Active SA BARS, where standard operation procedure is shown next to each point in the rating scale. The SA BARS is this research has been identified and developed using group of security experts who participated directly during the pilot. The Standard operation procedures for the

giving anchors were also identified as cyber security experts participated during the process. In Chapter 4 of this study covered that the quality and agility variables are the measure of SA performance. Therefore, Active SA BARS used these variables to in order to determine the participants SA performance. Active SA BARS used in this research to objectively measure and capture participants SA performance toward cyber incidents. This rating scale is completed by the researcher through examining participants answers to the questions discussed in section 3.12.2 and these answers are mapped into the scenario and experiment kill chains (Table 3.9) that participants are involve in. Active SA BARS is an objective measures developed and guided by the result extracted from the structural model of active SA explained in Chapter 4, section 4.5.4, where SA factor variables, quality and agility factor variables, and intelligence-related variables used from the structural model to evaluate the active SA theory in practice. Chapter 5 of this research shows the analysis where this rating scale is applied and the data from this and subsequently analysed using the t-test and ANOVA analysis to determine how well active SA group compared to the passive SA group performed in the experiment.

Table 3.9: Active SA BARS

			SOP(Passive)	*SOP(Active)*
Perception	***The correctness of the perception***	***Correctness***		
		1- Failed to perceived		
		2- Perceived false data	P	
		3- Perceived some of the truth but not sufficient to deter incident	P	
		4- Perceived some of the truth but sufficient to deter incident	P	A
		5- Perceived correct data		A
	The completeness of the perception	***Completeness***		
		1- Participant failed to detect suspicious activities		
		2- Perceived unrelated data	P	
		3- Perceived incomplete data but not sufficient to deter cyber incident	P	
		4- Perceived incomplete data and it is enough to deter incident		A
		5- Participant managed to get clear picture of the suspicious activities		A
Comprehension	***Participant analysis capability***	***Analysis***		
		1- Failed to understand what's going on in the network		
		2- Wrong judgement toward understanding the situation	P	
		3- Part of the truth has been identified, where participants failed to provide clear picture of the situation	P	
		4- Successfully understood the situation		A
		5- Clear understanding of the situation and willingness to take action		A
	Participant comprehension	***Confidence***		
		1- Participants failed to come up with a correct conclusion toward the situation		

		2- Hesitation to take action	P	
		3- Several hypotheses has been made	P	
		4- High self confidence toward participant finding		A
		5- trust in participant finding and willingness to take action		A
SA quality	***The accuracy of captured information***	***Accuracy***		
		1- Failed to capture the truth		
		2- Part of truth has been captured but with wrong judgement	P	
		3- Part of truth has been captured with successful judgement	P	
		4- Accurate information has been captured		A
		5- Participant managed to captured accurate information that allowed him to predict future		A
	The reliability of captured information	***Reliability***		
		1- Failed to capture reliable information		
		2- Non reliable information has been used that leads to poor judgement	P	
		3- Semi reliable information has been captured	P	
		4- Reliable data has been captured		A
		5- Captured information were reliable enough to predict future and control cyber incidents		A
	The timeliness of captured information	***Timeliness***		
		1- Failed to provide the information		
		2- Information has been provided after the cyber incidents	P	
		3- Information has been provided during cyber incidents	P	
		4- Information has been provided during cyber incidents where incident can be controlled		A
		5- Information has been provided before cyber incidents		A
SA agility	***Timeliness of awareness building***	***Timeliness***		
		1- Failed to provide SA		

	2- Partial of SA has been achieved after cyber incidents	P	
	3- Partial SA has been achieved during cyber incidents	P	
	4- SA has been achieved during cyber incidents		A
	5- SA has been achieved prior to cyber incidents		A
Capability to act	***Responsiveness***		
	1- Failed to response to cyber incidents		
	2- Response and action was not appropriate to cyber incidents	P	
	3- Response to cyber incidents was late	P	
	4- Proper response was in place during cyber incidents		A
	5- Proper response was in place prior to cyber incidents		A
Capability to adapt changes	***Adaptability***		
	1- Failed to adapt new measures		
	2- Not sufficient measure has been adopted	P	
	3- New measure adapted	P	
	4- Adaptability to new measure was in place during cyber incidents		A
	5- Adaptability to new measure was in place prior to cyber incidents		A

Usage of resources	***Security Controls***		
	1- Failed to utilise security dashboards		
	2- Used dashboards to find if there are suspicious activities after cyber incidents	P	
	3- Used dashboards to find there are suspicious activities during cyber incidents	P	
	4- Used dashboards to find the source of suspicious activities before execution of cyber attacks		A
	5- Utilisation of security controls to control cyber incidents (block or deceive)		A
	Deception		

1- No deception has been used	P	
2- Deception not used correctly		A
3- Deception used after cyber incidents		A
4- Deception used during cyber incidents		A
5- Deception used prior to cyber attacks		A
Blue Team		
1- Failed to utilise blue team	P	
2- Poor and unclear commands were given to blue team		A
3- Normal passive orders were given to blue team		A
4- Active and offensive orders were given to blue team after cyber incidents		A
5- Active and offensive orders were given to blue team during cyber incidents		A
Intelligence Report		
1- Did not rely on it	P	
2- No confidence in using it		A
3- Checked its validity through exploring dashboards		A
4- Confident in taking action		A
5- Used it without hesitation		A

3.2.6.11 Overall participant SA measurement method

The significance of measuring the efficiency, efficacy and effectiveness of the participants' SA performance with regard to new systems rests on the fact that the largest gap in current research is in how to perform situation projection, or, rather, to anticipate what to do in a sudden situation (Tadda, 2008). Such a state of affairs not only demands the application of collective knowledge, but also the synchronisation of efficiency, efficacy and effectiveness among the group of operators engaged in manning a particular network. The importance of measuring the above qualities in the participants in this research becomes even clearer if one extends the connotation of group synergy into a kind of fully aligned SA agility and SA quality among the group of operators.

It has already been observed that SA projection involves extensive use of tacit and explicit knowledge, and it is virtually impossible for team members to go for such knowledge exchange unless all of them are attuned to one another in terms of efficiency, efficacy and effectiveness. For that matter, it is crucial to measure individual levels of those elements, since this knowledge would enable the network management to underpin the individual advantages and disadvantages of the operators and to work on tuning the same for optimising their real-time SA performance (Endsley, 2000).

Furthermore, the security factor of a network also requires measuring the efficiency of the operators, since there is very little margin for error in managing a cyber attack. In fact, all instances of cyber attacks can be attributed to the lack of appropriate SA projection, which in turn can be attributed to a lack of team synergy, typically caused by the failure of the network's management to estimate the capacity and capability of the individuals who were given the charge to protect the network, where even the attitude of the operator is considered a crucial factor (Tadda, 2008).

Performance measures are based on tactical performance during missions and/or exercises, and accordingly the Situation Awareness Global Assessment Technique (SAGAT) (Endsley 2000), provides an objective measure of individual SA performance, covering all levels of SA, namely perception, comprehension and projection, to provide an accurate measure of an operator's SA. It also covers and reflects on the wide range of an operator's SA requirements that are derived from a goal-directed task analysis, which in turn underpins the operator's goals, the decisions that must be taken to achieve those goals, and the information needed by the operator for decision making. Successful validation of SAGAT through various tests (Endsley, 1989a, 1989b) clearly posits the fact that there exist differences in individual SA performance, and measuring tools like SAGAT can help in identifying and improving the SA performance of an individual. Therefore, it is important to build a measurement scale for active SA model that would allow observers to objectively measure the performance (efficiency, efficacy and effectiveness) of participants' SA. Using statistics and the SEM results in this research is the main source for the measurement scale adopted as the metrics used in this research relied on the result of exploratory factor analysis and SEM. The following part of this chapter will discuss this approach in detail.

In this research, exploratory factor analysis was conducted, as discussed in Chapter 4 section 4.4. This analysis confirmed the existence of five factors that makes active SA model. Also, confirmatory factor analysis, discussed in Chapter 4, confirmed that all factors are critical for building an active cyber SA. In addition, the structural model achieved for active cyber SA discussed in Chapter 4, section 4.5.4, Figure 4.4 reveals the causality that confirms the existence of strong causality and the criticality of all factors. The causality model of SEM determines the criticality and causality for achieving enhanced cyber SA and evaluating the overall cyber SA. Since all factors are critical success factors, and are essential for evaluating and achieving active cyber SA, it means all are needed and one cannot be prioritised above any other. Therefore, they all make an equal contribution to active cyber SA, very much like summative scale. In this research, the contribution of each factor was given equal rank because all factors are critical to overall cyber SA, and because they all impact on each other directly and indirectly, as shown in Figure 4.4 of Chapter 4. Also, the model discussed in this research is a thinking framework, and should be used by a cyber commander as guidance rather than as a process model. This is due to fact that active cyber SA is a mixture of all types of intelligence, technology and people involvement in understanding and building awareness regarding cyber incidents. If we take the case of cyber commanders, active cyber SA models allow a commander to request more active intelligence regarding an intelligence that comes from either local passive controls or other non cyber intelligence; thus, due to such interdependency of the model factors and their equal critical importance to the model, it is not possible to rank the factors. Therefore, an equal contribution was given to each of the active cyber SA model factors.

Variables weight is measured using the results of factor loading extracted from exploratory factor analysis, discussed in Chapter 4, Table 4.5. The weight during the development of the measurement scale was measured as described above, using the following equation:

$$\text{Weight} = 100 \,.\, \sum_{i=1}^{I} \left(\frac{FL_I}{\left| \sum_{vi=1}^{VI} FL_{vi} \right|} \right)$$

I: Number of variables
FL_I : Variable factor loading
FL_{VI}: Total factor loading

Example:
Quality and agility

X= Sum (factor loading) = 4.733

ES1 (timeliness of captured information) = (.944/4.733) 100 = 19.94506655*

Variables	Loading	Weight
ES3	0.944	19.94506655
ES2	0.857	18.10690894
ES4	0.798	16.86034228
ES5	0.752	15.88844285
ES7	0.7	14.78977393
ES1	0.682	14.40946546
	Total 4.733	

Table 3.10: Techniques to Measure Variable Weight

Total SA can be measured by the sum of each observed item of the factor's variable $Item_{IVF}$ captured from the participant SA multiplied by the weight of the factor's variable W_{VF} measured using the factor loading as describe previously, then divided by the total number of observed items of the factor's variable $|Items_{VF}|$. Regarding to SA efficiency, the formula will be the same as total SA, except the sum of each observed item of the factor's variable $Item_{IVF}$ will be replaced with the sum of each observed item describing the efficiency $EItem_{IVF}$ of the factor's variable, and this applies to the SA efficacy and SA effectiveness.

$$Total\ SA = \sum_{i=1}^{F} C_F . \left(\sum_{j=1}^{V_F} \left(\sum_{k=1}^{IV_F} Item_{IVF} . \left(\frac{W_{VF}}{|Items_{VF}|} \right) \right) \right)$$

F: Number of analysed factors.
C_F: Factor contribution.
V_F: Number of analysed variables per factor.
IV_F: Number of items per variable.
$Item_{IVF}$: Score of observed items per variable.
W_{VF}: Observed variable weight measured by the factor loading.
$Items_{VF}$: Total number of observed items per variable.

$$SA\ Efficiency\ = \sum_{i=1}^{F} C_F . \left(\sum_{j=1}^{V_F} \left(\sum_{k=1}^{IV_F} EItem_{IVF} . \left(\frac{W_{VF}}{|Items_{VF}|} \right) \right) \right)$$

$EItem_{IVF}$: Score of observed efficiency item per variable.

$$SA\ Efficacy\ = \sum_{i=1}^{F} C_F . \left(\sum_{j=1}^{V_F} \left(\sum_{k=1}^{IV_F} ECItem_{IVF} . \left(\frac{W_{VF}}{|Items_{VF}|} \right) \right) \right)$$

$ECItem_{IVF}$: Score of observed efficacy item per variable.

$$SA\ Effectiveness = \sum_{i=1}^{F} C_F . \left(\sum_{j=1}^{V_F} \left(\sum_{k=1}^{IV_F} EFItem_{IVF} . \left(\frac{W_{VF}}{|Items_{VF}|} \right) \right) \right)$$

$EFItem_{IVF}$: Score of observed effectiveness item per variable.

Cyber SA should be measured based on knowing the impact of each variables on cyber SA. This was achieved in this research by examining the results of exploratory factor analysis, confirmatory factor analysis and SEM. This value tells how much each variable contributes to the cyber SA model, and how much it explains the model. Therefore, using such techniques in this research it is possible to determine the real contribution of each variable to participants' cyber SA, and therefore the cyber SA was objectively measured. Table 3.11 shows the active SA measurement technique that contains the set of items describing each factor. Also, the table shows a colour coding for a set of items describing the

items that contribute to measuring (SA efficiency (red), SA efficacy (purple) and SA effectiveness (blue)).

This measurement metric was developed and guided by the results extracted from the structural model of active SA theory discussed in Chapter 4 and subject matter experts were used to identify the items which has been validated through the pilot. The variables used in this metric are those variables that this research used to evaluate cyber SA, which were again extracted from the structural model. Also, the items in these metrics were derived based on the scenario's ground truth, as explained in section 3.2.5 and 3.2.6, where participants' scores in SA BARS, SA-related questions answers and researcher observations helped in filling these metrics to extract the overall cyber SA performance. The results from this metric are used later, in Chapter 5's analysis, to determine how good the active offensive posture is in enhancing cyber SA.

Table 3.11: Active SA measurement metrics:

Weight		
14.7897739	Timeliness of Captured Information	0 or 1
	Detecting Network Scanning within 1 min	1
	Detecting Fingerprinting within 1 min	1
	Detecting Attack Execution within 30 sec	1
	Information about attack provided within 2 min	1
	Total	4
14.4094654	Timeliness of Awareness Building	0 or 1
	Data have been perceived within 90 sec	1
	Data have been analysed with 90 sec	1
	SA and projection achieved with 2 min	1
	SA achieved correctly within 2 min	1
	Total	4
18.1069089	Response	0 or 1
	Response was enough to deter cyber incidents	1
	Effective utilisation of resources in incident response	1
	Proper Action made within 2 min	1
	Total	3
19.9450665	Adaptability	0 or 1
	Changes to network were sufficient	1
	Changes to network were made within 2 min	1
	Total	2
16.8603422	Accuracy of Captured Information	0 or 1
	Scanning was Detecting within 1 min	1
	Source IP of attack was detected within 1 min	1
	Attacking port was identified within 1 min	1
	Attack type identified within 1 min	1
	Accurate Intelligence was provided	1
	Total	5
15.8884428	Reliability	0 or 1
	SA achieved and reliable to deter cyber incidents	1
	SA achieved and reliable to deter cyber incidents within 2 min	1
	Total	2
14.7605924	Perception Correctness	0 or 1
	Scanning was detected	1
	Source IP of attack was detected	1
	Attacking port was identified	1
	Attack type identified	1
	Intelligence was perceived within 2 min	1
	High self confidence toward intelligence	1
	Intelligence was perceived correctly	1

	Total	7
13.9166379	Perception Completeness	0 or 1
	Network scanning detected	1
	Attacker IP identified	1
	Type of attacks identified	1
	Attacked service identified	1
	Intelligence was provided within 2 min	1
	Provided intelligence was complete	1
	Total	6
15.3461935	Analysis	0 or 1
	Captured data analysed correctly	1
	Captured data analysed correctly and within 2 min	1
	Total	2
28.4877712	Comprehension	0 or 1
	Correct conclusion was made	1
	Data captured were analysed and understood within 2 min	1
	Total	2
27.4888046	Utilisation of Resources	0 or 1
	Utilisation of the deception service made correctly	1
	Utilisation of blue team offensive capabilities to extract intelligence	1
	Utilisation of security dashboards to validate provided intelligence	1
	Capabilities to focus into cyber incidents without ignoring cyber network	1
	Steady actions and responses to cyber incidents were made with confidence	1
	Total	5

Total SA value in %	100.000	Total SA %
SA Efficiency Value %	49.96	100.00
SA Efficacy Value %	16.48	100.00
SA Effectiveness Value %	35.56	100.00

3.3 Conclusion

The aim of this research is to investigate whether an active offensive hacking method is more capable of enhancing cyber SA agility and quality than the existing SA models. This aim stems from an ultimate aim of contributing to understanding the concept of cyber situational awareness.

This study adopts positivism as its research approach, while opting for mixed methods to avail of its proven advantages in the area of information systems. Altogether, the study manifested itself through two stages: in the first stage it collected data using an electronic survey, which was quantitative in nature; in the second stage it used the results of the SEM to design and develop the serious gaming environment with qualitative and quantitative instruments to test the effectiveness, efficacy and efficiency of active SA. Accordingly, the Structure Equation Modelling (SEM) was used in the first stage to verify the hypothesised theoretical model and test the estimate and causal relations, and its outcome was then used in the second stage to develop the SA awareness behavioural anchor-rating scale, and the SA measurement and marking scheme based on ground truth.

A clear justification has been provided within this chapter regarding the methods selected, and has shown how these methods are best suited to this research study. This research has three methodological contributions. First, this research provided techniques to measure the variable weight using the factor loading extracted from exploratory factor analysis. Second, design and develop an objective quantitative SA measurement metrics based on the result of SEM which provided a novelty as this method this research the ability to quantify SA. Finally, the development of the Serious Gaming Environment (SGE) enabled the validation of the research theory against real world physical networks and network assets in a small, controllable environment. The scenario chosen was the Abu Dhabi Securities Exchange, and this allowed for further, more detailed validation against the specific nuances of the ADX scenario involving the research on a more granular level.

CHAPTER 4: DATA ANALYSIS (SEM): ASA THEORETICAL DEVELOPMENT

4.0 OVERVIEW

This chapter analyses the SEM results of the theoretical model introduced in Chapter 2, designed to test the suggested hypotheses between the underlying constructs in the ASAM. Hair et al. (2006) suggest using different elementary tests as guides before conducting the two phases for testing the proposed framework. Primarily, the measurement model should be tested; this model helps to describe the link between the items observed and the unobserved (latent) construct. Furthermore, this phase specifically highlights the findings of the confirmatory factor analysis. The structural model is tested in the second stage, which seeks to describe the causal links between the recognised constructs. The following parts of this study describe the analyses and the findings of the tests. More detail is included in appendix 2.

4.1 SAMPLE AND PROCEDURE

A quantitative approach was adopted for the current research in order to test the proposed model (Figure 1). A non-probabilistic sample was collected and can be considered as suitable for our research purpose. An electronic survey was used because of its various advantages, specifically in that it is possible for it to reach a wider audience, thus allowing a larger sample to be obtained for further analysis. Specifically, a self-administered questionnaire containing 42 questions was used to collect empirical data. The target sample for this survey was cyber security experts from different countries recognised as top ranking experts in cyber security, but mainly focusing on CERT's personnel locating in the US, the UK, the EU and the UAE. Participation was on a voluntary basis, and no financial incentives were offered. A total of 600 self-administered questionnaires were distributed to the experts; the number of completed questionnaires returned was 312.

4.2 DATA PREPARATION

4.2.1 Data Coding and Editing

In an attempt to ensure data consistency and comprehensiveness following data gathering, data editing was performed (Tabachnick & Fidell, 2007). Of note, this study comprises only respondents who successfully answered all the questions asked. Any data seen to be missing or incomplete have not been taken into account. Throughout the coding methodology, this study assigned each question answered with a specific number, which was then inputted into an SPSS file for statistical analysis. Following the coding of the data, this researcher carried out editing in order to ensure the effective completion of the coding process. In addition, for any value seen to be out of range, a validation of that value was assessed by reverting back to the original questionnaire.

4.2.2 Data Screening

In the attempt to ensure that all data were properly and accurately entered, and that all variables were normally distributed, data screening was carried out. The aim was to establish whether or not there were any missing data, normality issues and/or outliers. The following sections describe this initial analysis.

Treatment of Missing Data and Unengaged Responses

Two different approaches have been described by Tabachnick & Fidell (2007: 62-63) in order to address the issue of missing data; i.e. when respondents do not successfully answer one or more of the survey questions. The primary approach is linked with the pattern of missing data, involving the researcher establishing the source of the missing data in line with non-random or random (i.e. related to specific items) occurrence. Otherwise stated, should the missing data be distributed randomly throughout the questionnaire, there would then be a lack of researcher bias. However, if the missing data were distributed throughout the questionnaire in a non-random way, this could impact on the overall generalisability and wider impact of the findings. The second approach is associated with the volume of data missing. Although the previously highlighted approaches are noted by Tabachnick & Fidell (2007), the point is nevertheless made that patterns of missing data are extremely more valuable than the volume of data found to be missing. In this study, data screening highlighted less than 5% missing values for all of the constructed questions; this percentage is regarded as acceptable (Churchill, 1979). Missing-data randomness was evaluated in an attempt to ensure that no systematic errors were present (Hair et al., 2006). This study, as explained earlier, only accepted completed surveys, so no data treatment was required.

In this study, 27 records with missing data were found, which accounted for 10% of all data. In an attempt to handle this situation effectively, the decision was made to delete these data based on the reasons discussed above. Specifically, three rows of questions were found to have missing data only in three questions; the most common response was utilised as a replacement, but the decision was to remove them from any further analysis.

The unengaged response is the result of the zero standard deviation of a series, meaning that all of the series' numbers are equal to the mean value of each of the numbers included in the series. Through the exercise of the survey, 14 rows had a standard deviation close to zero. Owing to the fact that this showed no variance, the decision was made to delete these data to avoid issues in SEM analysis.
The final sample size contained 271 responders with clean and complete data (N = 271).

4.3 Assessment of Normality, Linearity, Multicollinearity, Outliers and Cronbach's Alpha for Active Situational Awareness Model

4.3.1 Normality

A normality test was completed in order to ensure that data did not violate the normality assumption. Attention was directed to the Jarque-Bera (skewness-kurtosis) test in order to ensure that all the constructs were within the acceptable limit of the skewness-kurtosis ranges (Table 4.1). The skewness-kurtosis test draws a contrast between the study data distributions and normal distribution (Hair et al., 2006). In one regard, skewness is able to deliver some insight into the symmetry and balance of the distribution, such as whether or not the distribution has shifted to a particular side. For instance, if there is a positive skew in the distribution (i.e. if the values are grouped to one side), this suggests a positive outcome/relationship. Kurtosis also delivers insight into the distribution height, referred to as 'peakedness' or 'flatness'. In this regard, positive values suggest peaked distribution, whilst a flatter distribution is seen through a negative kurtosis (Hair et al., 2006: 80). Skewness-kurtosis critical values have been discussed and examined by many different academics (Hair et al., 2006; Tabachnick & Fidell, 2007) and should be within the range of ± 2.58 at the 0.01 significance level. The skewness and kurtosis values of the constructs, shown in Table 4.1, were within these critical values, confirming that the data (univariate) were normally distributed.

Table 4.1: The Mean, Standard Deviation, Variance, Skewness and Kurtosis of the Study Constructs

Construct	N	Mean		Std. Deviation	Variance	Skewness		Kurtosis	
	Statistic	Statistic	Std. Error	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
IG	271	2.151	0.04342	0.71471	0.511	0.813	0.148	0.936	0.295
PI	271	3.0418	0.04465	0.73506	0.54	-0.082	0.148	-0.119	0.295
AI	271	3.3512	0.04205	0.69231	0.479	-0.481	0.148	0.465	0.295
SA	271	3.809	0.03498	0.57581	0.332	-0.731	0.148	1.321	0.295
QA	271	3.9263	0.03767	0.62018	0.385	-0.632	0.148	1.305	0.295

4.3.2 Linearity and Multicollinearity

To examine the linearity of relationships between variables, this study utilised the bivariate correlation matrix at the 0.01 significance level (2-tailed) in an attempt to establish the linearity and multicollinearity of the Active Situational Awareness Model (ASAM) constructs. As can be seen in Table 4.2 below, a very low correlation with the independent variables was observed (Pearson's correlation, r, is below 0.7), thus confirming that multicollinearity between ASAM constructs is not probable.

Table 4.2: ASAM Constructs Correlation and Pearson's Correlation

	IG	PI	AI	SA	QA
IG	1				
PI	.419**	1			
AI	.256**	.608**	1		
SA	.297**	.406**	.532**	1	
QA	.231**	.367**	.465**	.647**	1

**. Correlation is significant at the 0.01 level (2-tailed).

4.3.3 Outliers

Outliers are described as being the most extreme points of data that can greatly impact on the SEM, and thus on the overall findings and conclusions. Outliers are typically observed due to errors that may arise when respondents respond to subjects, or because of erroneous data recording. Furthermore, there may be instances of outliers when the various respondents represent a different population from the study population under examination. Corrective actions geared towards minimising outliers include data validation and correction (at the extremes), removal of the extreme data, definition of the population in question, or compilation of a model re-specification. Nevertheless, the corrective measure ultimately rests on the outlier's source. Identifying an outlier through observation is neither simple nor straightforward, even if the data sample is large. One of the most common approaches to recognising outliers involves the boxpot outlier-labelling rule, initially presented by Tukey (1977), which has subsequently been altered and adapted into a proper outlier identification rule through the work of Hoaglin & Iglewiez (1987). Through the application of this rule, observations are recognised as outliers when they are found beyond the interval shown below.

$$Q_1 - g(Q_3 - Q_1),$$

$$Q_3 + g(Q_3 - Q_1),$$

Hoagin et al. (1986)

Where Q_1 and Q_3 is the value of 25% and 75% respectively (Boris & Sharmila, August, 2001)

Initially, the most widely used choice for g was 1.5, but observations have been flagged up with 3.0, after Hoagin et al. (1986) found issues with a g value of 1.5. This rule does not depend on the size of the sample; thus, it can vary from the standard outlier identification rule, positioned at a certain probability of outliers, or with none existing. Hoagin et al. (1987) then provided evidence for the fact that a g value of 2.2 was the most suitable choice; for the purposes of our research, this recommendation was applied.

In this study, it was established through the test that there were no outliers using the equation shown below. Moreover, the highest values did not exceed that of the upper limit, whilst the lowest value did not fall below that of the lowest value calculated. (Check Appendix 2).

For the upper quartile $u^3 = Q_3 + (2.2(Q_3 - Q_1)$

Whilst for the lower quartile $u^1 = Q_1 - (2.2(Q_3 - Q_1)$

4.3.4 Cronbach's Alpha

Cronbach's alpha is recognised as a construct reliability or consistency coefficient, but ultimately it is not a statistical test. A reliability coefficient of ≥ 0.70 is considered acceptable in social science study analysis (Bollen, 1989). Importantly, all of the values are seen to be greater than 0.7 when conducting the test, implying that the scale is reliable. In the following part, further insight will be given.

4.4 FACTOR ANALYSIS (EXPLORATORY FACTOR ANALYSIS)

The main extraction method of this study is a maximum likelihood factoring approach, a form of common factor analysis, for a number of different reasons (Hair et al., 2006). Primarily, when drawing a contrast between a maximum factor likelihood approach and a principal factor approach, known to be another type of common factor analysis, there are desirable asymptotic properties supporting the former (Bickel & Doksum, 1977). Indeed, the majority of statisticians prefer maximum likelihood factor analysis because it requires a multivariate, normal distribution (Geweke & Singleton, 1980). In addition, whereas principal factor analysis takes into account the total variance (i.e. common, unique and error variances), maximum likelihood factor analysis is concerned with the common variance (Hair et al., 2006; Tabachnick & Fidell, 2007). Finally, the maximum likelihood factoring approach considers the correlation matrix as a sample correlation matrix, with Fabrigar et al. (1999, p. 277) postulating that, should the data be distributed relatively normally, the maximum likelihood factoring approach is the most appropriate choice as it permits: 1) calculation of a number of different indexes of goodness of fit; 2) statistical tests of correlations and factor loadings between factors to be performed; 3) calculation of confidence intervals. Appendix 2 of this study contains all the test result in detail.

The creation of a correlation matrix was done to ensure the reliability of and test the links between the constructs. The findings associated with the bivariate correlation matrix highlighted that the constructs were not highly correlated with one another (r was below 0.7, indicating that multicollinearity is unlikely; see Table 4.2). Furthermore, the pattern matrix findings (exploratory factor analysis, Table 4.5) emphasised that the constructs were not cross-loaded, suggesting that there was a distinction to be recognised between constructs. In addition, the confirmatory factor analysis findings confirmed that cross-loading between constructs was impossible, with each construct united alongside its own associated items (tables 4.10-4.14). Lastly, a discriminant validation analysis was carried out in order to ensure that constructs stood alone and did not interact with any other (Table 4.15).

It has been suggested by Field (2005) that three tests should be performed in order to establish the overall adequacy of the extraction approach in the context of factor analysis: 1) the Kaiser-Meyer-Olkin (KMO) test of sampling adequacy; 2) eigenvalue; 3) Bartlett's test of sphericity. With the aim of establishing whether or not factor analysis extraction methods are considered acceptable, Field (2005) postulates that, if the amount of variables utilised in factor analysis is lower than 20 and the sample size is above 250, the average communality is equal to or greater than 0.6 and the Bartlett's test of sphericity is significant, then factor analysis extraction is acceptable. Importantly, the conditions mentioned earlier, notably that the KMO of sampling adequacy is 0.923 ($\geqslant$0.6 is acceptable in the view of Tabachnick & Fidell, 2007) and that the Bartlett's test of sphericity is significant ($p < 0.001$), have been adhered to in this study. Indeed, the results obtained from Bartlett's test of sphericity and the KMO (Table 4.3) helped to validate the overall factorability of the correlation matrix, as the results confirmed that factor analysis was the most suitable option. Furthermore, the initial five elements explained more of the variation than the other remaining factors. To validate this finding, this study carried out reproduced correlations for the percentage of non-redundant residuals with an absolute value >0.05. Notably, (Table 4.6) the percentage was recognised as being considerably lower than 50%, with a final score of 8%, thus, there was no requirement for the retention of additional factors.

Table 4.3: KMO and Bartlett's Test

Kaiser-Meyer-Olkin's Measure of Sampling Adequacy		0.923
Bartlett's Test of Sphericity	Approx. Chi-Square	7687.833
	df	595
	Sig.	0

Table 4.4: Goodness-of-Fit Test

Chi-Square	Df	Sig.
944.284	430	0.000

4.4.1 Factor Loading

This study adhered to the guidelines provided in the academic literature (e.g. Hair et al., 2006; Tabachnick & Fidell, 2007) for establishing the most suitable loading between a variable and its associated factors (i.e. for each variable on each factor). In line with the guidelines presented by Hair et al. (2006) for establishing a significant factor loading, and in accordance with the sample size of this study (n = 271 cyber experts), the most suitable factor loading was recognised as 0.35 and above, at the 0.05 significance level (see Table 4.5). Throughout the course of the test, three different variables were seen to demonstrate a low extraction (in 20, 21 and 22), which were recognised as potentially causing an issue through CFA. The choice was centred on retention, thus enabling greater examination at a later date.

The findings obtained through the rotation approach emphasised that SPSS rotated five factors, with all the loadings identified as being more than 0.35. The pattern matrix (see Table 4.5) shows the five individual rotated factors: 1) the Situational Awareness construct, which accounted for 34.775 of the total variance; 2) the Quality and Agility construct, which was responsible for 10.33% of the total variance; 3) the Active Intelligence construct, which explained 9.724% of the total variance; 4) the Passive Intelligence construct was 6.153% of the total variance; 5) the Intelligence Gathering construct, which accounted for 5.003 % of the total variance (64.984%) (see Table 4.6).

Table 4.5: Rotated Component Matrix. Pattern Matrix variable listed is labelled in section 3.12.2

Variables		Factor				
		SA	Quality & Agility	Active Intelligence	Passive Intelligence	Intelligence Gathering
Skill	S4	.919				
Previous knowledge	S3	.904				
Analysis Capability	S5	.891				
Perception Correctness	S1	.857				
Perception Completeness	S2	.808				
Confidence	S6	.750				
Projection (intent)	S7	.677				
Adaptability	ES3		.944			
Responsiveness	ES2		.857			
Quality Accuracy	ES4		.798			
Quality Reliability	ES5		.752			
Quality Timeliness	ES7		.700			
Timeliness	ES1		.682			
Enemy Possible Attack	in21		.562			
Granular Level of Threat Detail	in20		.558			
Enemy Attack Timing	in22		.490			
Active Intelligence Gathering Capability	in14			.941		
Information Gathering	in12			.867		
Destroy	in13			.865		
Enemy Weaknesses	in9			.862		
Intelligence Completeness	in11			.831		
Intelligence Accuracy	in10			.742		
Enemy Capabilities	in8			.616		
Intelligence Collaboration	in6				.878	
Intelligence Sharing	in5				.861	
Enemy IP	in2				.853	
Passive Intelligence Gathering Capability	in4				.773	
Enemy Motive	in3				.757	
Intelligence Timeliness	in1				.641	
Interaction Capability	in7				.574	
Enemy Geo Location	in17					.914
Enemy Attack Variation	in18					.867
Non Cyber intelligence	in16					.867
Enemy Attack Consistency	in19					.866
Resources Availability	in15					.741

Table 4.6: Total Variance Explained

Factor	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1(SA)	12.611	36.030	36.030	12.171	34.775	34.775	8.744
2(QA)	4.058	11.593	47.623	3.615	10.330	45.104	8.278
3(AI)	3.285	9.387	57.010	3.053	8.724	53.828	8.531
4(PI)	2.471	7.061	64.071	2.153	6.153	59.981	7.693
5(IG)	2.001	5.718	69.789	1.751	5.003	64.984	5.339
6	.847	2.420	72.209				
7	.767	2.192	74.401				
8	.668	1.909	76.310				
9	.650	1.858	78.168				
10	.631	1.803	79.972				
11	.594	1.697	81.668				
12	.531	1.518	83.186				
13	.486	1.389	84.576				
14	.434	1.241	85.817				
15	.417	1.192	87.009				
16	.381	1.089	88.098				
17	.377	1.076	89.174				
18	.345	.985	90.159				
19	.338	.965	91.124				
20	.322	.920	92.045				
21	.291	.831	92.875				
22	.279	.798	93.674				
23	.252	.721	94.394				
24	.231	.659	95.053				
25	.214	.612	95.665				
26	.202	.578	96.243				
27	.193	.551	96.794				
28	.177	.505	97.299				
29	.166	.473	97.773				
30	.165	.471	98.244				
31	.151	.432	98.676				
32	.142	.406	99.082				
33	.125	.356	99.438				
34	.110	.314	99.752				
35	.087	.248	100.000				

4.5 Analysis and Results of the Structural Equation Modelling (SEM)

This study utilised SEM with the aim of testing the hypotheses between the underlying constructs in the ASAM. Hair et al. (2006) suggest that two individual phases can be utilised in order to test a proposed framework with the use of SEM. First, the measurement model should be tested; this model helps to describe the link between the items observed and the unobserved (latent) construct. Furthermore, this phase notably links the findings of the confirmatory factor analysis with the structural model tested in the second stage, which seeks to describe the causal links between the recognised constructs. The following parts of this study describe the analyses and the findings of the frameworks.

4.5.1 Measurement Model

Unidimensionality and goodness-of-fit criteria were adopted with the aim of assessing the overall measurement model and its criteria. In one regard, unidimensionality was examined through the application of reliability tests (i.e. composite and Cronbach's alpha reliabilities), with factor loadings adopted for all of the constructs but on an individual basis. In contrast, a number of goodness-of-fit criteria were selected in this study, as it was difficult to rely on only a single fit index when establishing the most appropriate framework (Byrne, 2001). This study centred on three different types of goodness-of-fit criteria, namely absolute, incremental and parsimony. In line with the study by Hair et al. (2006: 706-708), absolute fit indices are adopted when seeking to examine the overall goodness-of-fit for the measurement and structural frameworks collectively. Nevertheless, the absolute fit indices assess goodness-of-fit of a particular framework individually from another framework. Essentially, it may be stated that the incremental fit indices are adopted when evaluating how well a particular framework fits in line with a number of other, alternative baseline frameworks. Owing to the fact that the absolute fit indices do not draw a comparison between frameworks and a particular null model, this study utilised incremental fit indices as well as absolute fit. When possible, use of parsimony fit analysis was conducted in order to establish which of the models was most suitable (Hair et al., 2006). The table below provides an overview of the key goodness-of-fit criteria adopted in this study.

Table 4.7: Goodness-of-Fit Criteria Used in this Research

Fit Index	**Recommended Value (Hair, 2006)**
χ^2	Non-significant at $p < 0.05$
Degrees of Freedom (DF)	n/a
χ^2 /df	<5 preferable <3
Goodness-of-Fit Index (GFI)	>0.90
Adjusted Goodness-of-Fit Index (AGFI)	>0.80
Comparative Fit Index (CFI)	>0.90
Root Mean Square Residuals (RMSR)	<0.10
Root Mean Square Error of Approximation (RMSEA)	<0.08
Normed Fit Index (NFI)	>0.90
Parsimony Normed Fit Index (PNFI)	>0.60

4.5.2 Initial CFA Model

A good fit was not recognised through the initial framework (see Table 4.8 and Appendix 2). Taking into account various statistical parameters, the standardised residual covariance of some of the variables was not within the range of ± 2.58; the standardised regression weight of three variables identified earlier in section 4.4.1 (in20, in21 and in22) was less than 0.5; the SMC (squared multiple correlations) was less than 0.5. Moreover, the modification indices (MI) showed a high covariance, thus signifying high covariance. Accordingly, the decision was made to remove these variables in order to have a good model fit. Furthermore, the GFI was found to be lower than 0.9, with the AGFI less than 0.8, the CFI and NFI less than 0.9 and, finally, the RMSEA no less than 0.08. These parameters failed to fulfil the suggested measure, as shown previously in Table 4.7, and thus the model needed to be revised in order to achieve a satisfactory fit. Accordingly, the following measures were adopted to achieve required fit (Figure 4.2):

- The standardised residual covariance was adjusted to be within the range ± 2.58 (Byrne, 2006).
- Factor loading (standardised regression weight) needed to be larger than 0.5 and preferably above 0.7 (Byrne, 2006).
- The SMC value required to be larger than 0.5 (Byrne, 2006).
- The MI which revealed a very high covariance and demonstrated high regression weights should be omitted from further analysis (Byrne, 2006; Hair et al., 2010).

Table 4.8: Initial CFA Model Result

Fit Index	**Result**
x 2 /df	2.712
Goodness-of-Fit Index (GFI)	0.754
Adjusted Goodness-of-fit Index (AGFI)	0.719
Comparative Fit Index (CFI)	0.874
Root Mean Square Residuals (RMSR)	0.075
Root Mean Square Error of Approximation (RMSEA)	0.08
Normed Fit Index (NFI)	0.815
Parsimony Normed Fit Index (PNFI)	0.753

a. Acceptable Measurement Model

Figure 4.2: Measurement Model (Table 4.5) (Source: Author)

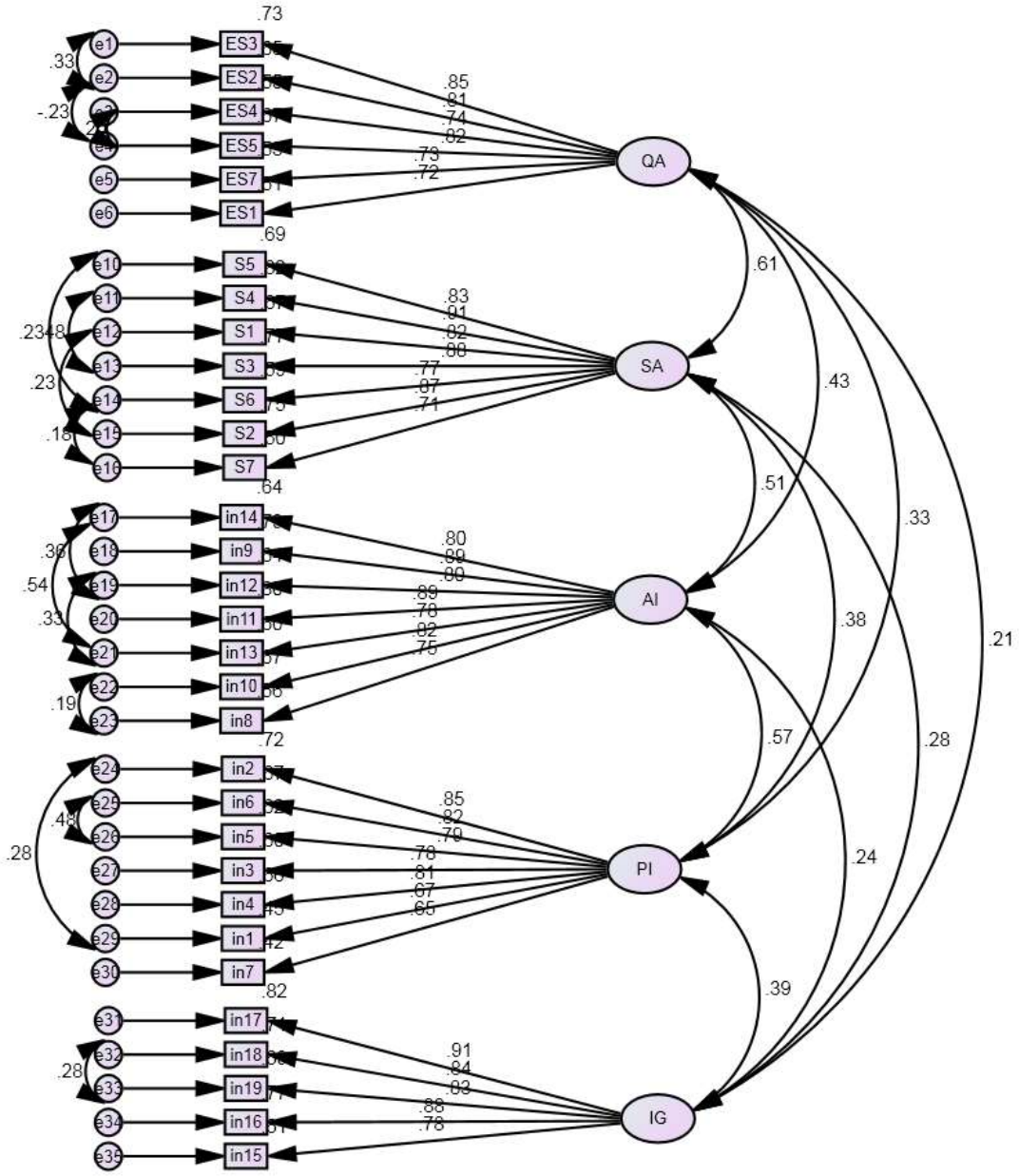


Table 4.9: Measurement Model Result

Fit Index	Result
χ 2 /df	1.558
Goodness-of-Fit Index (GFI)	0.868
Adjusted Goodness-of-Fit index (AGFI)	0.843
Comparative Fit Index (CFI)	0.965
Root Mean Square Residuals (RMSR)	0.032
Root Mean Square Error of Approximation (RMSEA)	0.045
Normed Fit Index (NFI)	0.908
Parsimony Normed Fit Index (PNFI)	0.813

Figure 4.2 displays a measurement model comprising 32 different indicators, whilst Table 4.9 provides a summary of the fit index results of the acceptable measurement framework. It is recognised that the GFI needs to be at least 0.9, which has not been achieved through this model (Hair et al., 2006); as other indexes showed a good fit, this study nonetheless recognised this framework as a good fit. The tables below, i.e. Table 4.10 through to Table 4.14, detail the findings of the measurement framework, including the standardised factor loadings (λ), estimates, standard errors (SE), critical ratios (CR), squared multiple correlations, average variance extracted (AVE), and composite and Cronbach's alpha reliabilities for all of the constructs of interest. The tables help to display a number of findings, as follows.

Each of the construct indicators' factor loadings was significant. The confirmatory factor analysis was, for all of the constructs, sufficient in the context of performing structural modelling, and was also found to be significant. The standardised factor loading (λ) had a value exceeding 0.70, which suggested a key link between the construct and its factors. The critical ratio (or t-values) was found to be over 1.96 for the entire factor loadings, which implied statistical significance, as recognised by Byrne (2001) and Hair et al. (2006). The AVE (Average Variance Extracted) highlighted the data relating to the amount of variance captured by the construct in regard to the variance degree owing to measurement error (Fornell & Larker, 1981: 45). AVE is also known to represent a greater indicator of the construct's reliability, as opposed to the composite's reliability (Fornell & Larker, 1981). The findings presented here illustrate that the average variance from the extracted values of all model constructs suggest a span from between 0.591 and 0.72; this surpassed the minimum value of 0.50 or more suggested by Fornell & Larker (1981). Composite reliabilities for all of the constructs ranged from 0.902 to 0.938, thus surpassing the minimum value of 0.70 suggested by Hair et al. (2006). Cronbach's alpha reliabilities for all of the constructs ranged from 0.903 through to 0.943, which also surpassed the minimum value of 0.70 suggested by Field (2005). Moreover, with the average variance extracted, Cronbach's alpha reliabilities and composite reliabilities signified acceptable levels of both validity and reliability suggested by Fornell & Larker (1981) and Hair et al. (2005). (Table 4.10-14)

Reliability Cronbach's alpha = .903				Composite reliability = .902					
Standard factor loading (λ)				Estimate	S.E.	C. R.	P	SMC	Average variance extracted
ES3	<---	QA	0.853	1				0.513	0.607
ES2	<---	QA	0.808	0.931	0.049	18.858	***	0.531	
ES4	<---	QA	0.742	0.899	0.067	13.323	***	0.666	
ES5	<---	QA	0.816	0.912	0.06	15.189	***	0.551	
ES7	<---	QA	0.728	0.837	0.063	13.364	***	0.653	
ES1	<---	QA	0.716	0.84	0.064	13.068	***	0.727	

Table 4.10: Agility and Quality Construct

Reliability Cronbach's alpha = .942				Composite reliability = .938					
Standard factor loading (λ)				Estimate	S.E.	C. R.	P	SMC	Average variance extracted
S5	<---	SA	0.83	1				0.504	0.685
S4	<---	SA	0.906	1.11	0.059	18.682	***	0.752	
S1	<---	SA	0.819	1.01	0.063	15.967	***	0.589	
S3	<---	SA	0.877	1.102	0.062	17.681	***	0.769	
S6	<---	SA	0.768	0.937	0.056	16.658	***	0.671	
S2	<---	SA	0.867	1.078	0.062	17.492	***	0.82	
S7	<---	SA	0.71	0.824	0.063	13.115	***	0.689	

Table 4.11: Situational Awareness Construct

Reliability Cronbach's alpha = .939				Composite reliability = .935					
Standard factor loading (λ)				Estimate	S.E.	C. R.	P	SMC	Average variance extracted
in14	<---	AI	0.8	1				0.641	0.672
in9	<---	AI	0.887	1.19	0.07	16.989	***	0.786	
in12	<---	AI	0.801	1.094	0.059	18.628	***	0.642	
in11	<---	AI	0.892	1.037	0.061	17.134	***	0.796	
in13	<---	AI	0.777	0.972	0.046	20.948	***	0.604	
in10	<---	AI	0.82	1.088	0.071	15.233	***	0.673	
in8	<---	AI	0.751	1.017	0.075	13.53	***	0.564	

Table 4.12: Active Intelligence Construct

Reliability Cronbach's alpha = .913				Composite reliability = .909					
Standard factor loading (λ)				Estimate	S.E.	C. R.	P	SMC	Average variance extracted
in2	<---	PI	0.85	1				0.722	0.591
in6	<---	PI	0.819	1.019	0.064	16.038	***	0.671	
in5	<---	PI	0.786	0.975	0.065	15.017	***	0.617	
in3	<---	PI	0.777	0.904	0.061	14.886	***	0.603	
in4	<---	PI	0.809	0.949	0.06	15.821	***	0.655	
in1	<---	PI	0.667	0.73	0.053	13.808	***	0.445	
in7	<---	PI	0.649	0.763	0.066	11.614	***	0.421	

Table 4.13: Passive Intelligence Construct

Reliability Cronbach's alpha = .928				Composite reliability = .928					
Standard factor loading (λ)				Estimate	S.E.	C. R.	P	SMC	Average variance extracted
in17	<---	IG	0.906	1				0.821	0.72
in18	<---	IG	0.841	0.982	0.051	19.094	***	0.708	
in19	<---	IG	0.831	0.937	0.05	18.594	***	0.69	
in16	<---	IG	0.877	1.154	0.055	20.988	***	0.769	
in15	<---	IG	0.782	0.986	0.059	16.766	***	0.612	

Table 4.14 Intelligence Gathering Construct

*** P-value < 0.001

4.5.3 Reliability and Validity of Constructs

As highlighted by various scholars (Hair et al., 2006; Fornell & Larckers, 1981), evaluating construct validity is an outcome of two component validities: convergent and discriminant.

a) Convergent validity

Convergent validity is associated with the internal consistent validity between all of the construct items, such as low or high correlations (Fornell & Larckers, 1981). In this research, convergent validity was evaluated in line with the indicators' estimated coefficients for all of the measurement scales (composite reliability), which included the average variance extracted as well as Cronbach's alpha. Interestingly, tables 4.10-4.14 help to illustrate that the composite reliability for all constructs exceeded 0.902, with an average variance of more than, or at least equal to, 0.5, whilst Cronbach's alpha was above 0.7. All these results were regarded as sound indicators of the convergent validity (Fornell & Larckers, 1981).

b) Discriminant Validity

Discriminant validity was carried out with the aim of ensuring that all of the constructs and their associated indicators in the suggested framework varied from others and their indicators. The discriminant validity for all of the ASAM model's constructs is summarised in Table 4.15; no validity concern was seen in the framework presented. Moreover, the diagonal line highlights the squared roots of average variance extracted (SRAVE) for all of the constructs, which is greater than any link value below it; this suggests an acceptable level of discriminant validity (Fornell & Larckers, 1981).

Table 4.15: Discriminant Validity

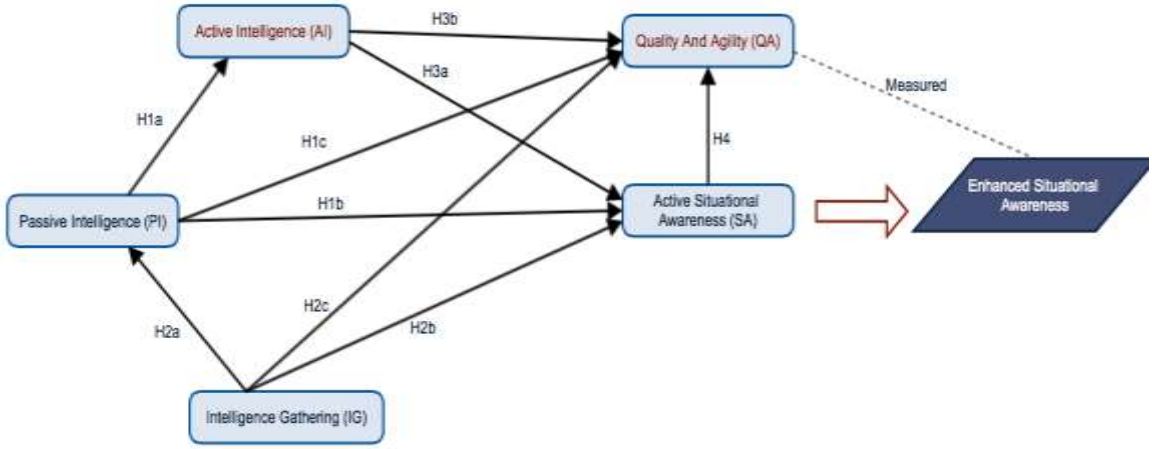
Construct	**CR**	**AVE**	**MSV**	**ASV**	**PI**	**QA**	**SA**	**AI**	**IG**
PI	0.909	0.591	0.319	0.182	0.769				
QA	0.902	0.607	0.366	0.177	0.335	0.779			
SA	0.938	0.685	0.366	0.211	0.380	0.605	0.828		
AI	0.935	0.672	0.319	0.205	0.565	0.431	0.506	0.820	
IG	0.928	0.720	0.152	0.084	0.390	0.212	0.282	0.240	0.848

4.5.4 Structural Model: Hypotheses Testing

The ASAM findings are described in Figure 4.3 and Figure 4.4. These findings of the suggested conceptual framework highlighted a chi-square of 691.547 (degrees of freedom, df = 444; $p < .001$), GFI of 0.868 (not >0.9, as recommended, but still an improvement on the initial 0.754), AGFI of 0.843, CFI of 0.965, NFI of 0.902, incremental fit index (IFI) of 0.965 and $\chi 2/df = 1.558$. Importantly, all of the indices showed a good model fit (e.g. AGFI, NFI, CFI and IFI should be equal to or greater than 0.9, according to Byrne, 2001 and Hair et al., 2006). Moreover, the RMSEA provided a value of 0.045 (notably, an acceptable level needs to fall below 0.08, in line with the suggestion of Hair et al., 2006). All fit indices established throughout the course of this study were recognised as being within the acceptable limits (Byrne, 2001; Hair et al., 2006; Tabachnick & Fidell, 2007).

Figure 4.4 details the final framework, comprising the coefficient of determination (R^2) and structural path coefficients. All the conceptual model hypotheses were statistically supported ($p < 0.001$). In addition, as emphasised in Table 4.16, the Intelligence Gathering (IG) construct highlighted a notably positive impact on the Passive Intelligence (PI) and Situational Awareness (SA) constructs (H2a: t = 7.577; H2b: t = 3.296). Interestingly, the PI construct had a significant and positive impact on the Active Intelligence (AI) construct (H1a: t = 12.582). The AI construct itself provided significant positive effects on the SA and the Quality and Agility constructs (QA; H3a: t = 9.346; H3b: t = 3.115). Finally, the SA construct provided a significant and positive impact on the QA (H4: t = 10.254).

Figure 4.3: The Theoretical Model and Research Framework (Source: Author)

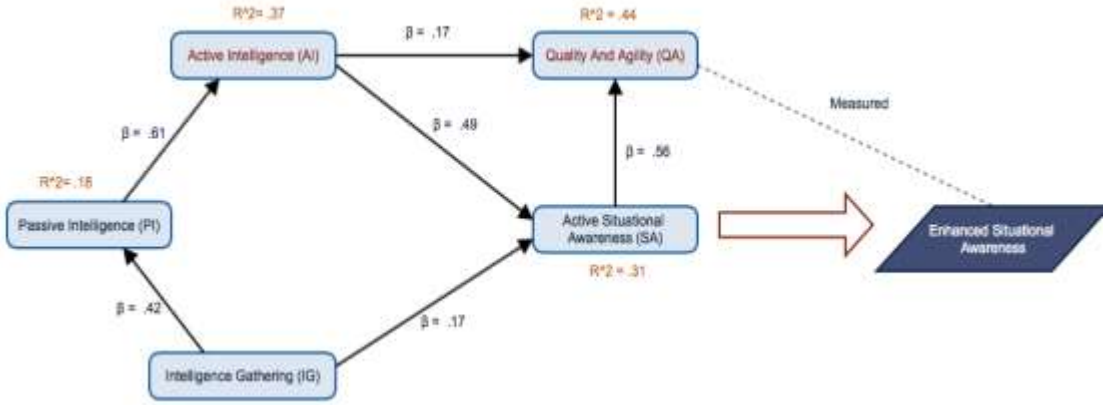


Model Hypotheses:

H1a: Passive Intelligence (PI) positively impacts on Active Intelligence (AI).
H1b: Passive Intelligence (PI) positively impacts Situational Awareness (SA).
H1c: Passive Intelligence positively impacts on the Quality and Agility of SA (QA).
H2a: Intelligence Gathering (IG) positively impacts on Passive Intelligence (PI).
H2b: Intelligence Gathering (IG) positively impacts on Situational Awareness (SA).
H2c: Intelligence Gathering (IG) positively impacts on the Quality and Agility of SA (QA).
H3a: Active Intelligence (AI) positively impacts on Situational Awareness (SA).
H3b: Active Intelligence (AI) positively impacts on the Quality and Agility of SA (QA).
H4: Situational Awareness (SA) positively impacts on the Quality and Agility of SA (QA).

The above qualitative model hypotheses were discussed earlier in chapter 2 section 2.5.1 where a conceptual hypothesise active SA model that shows the causal relations between the Active SA model constructs used as SEM required qualitative hypothesis. Therefore, the fitness of structural model can be determined and causal effect of each construct can be identified.

Figure 4.4: The Results of the Structural Model, the Standardised Path Coefficient between Constructs and R2 (Source: Author)



Where CMIN/DF (χ 2 /df) = 1.558, RMR = 0.032, GFI= 0.868, AGFI = 0.843, CFI = 0.965, NFI= 0.908, PNFI = 0.813, RMSEA = 0.045); P < 0.001.

Table 4.16: Hypotheses Testing

Standardised Regression Paths (β)		Estimate	S.E.	C.R.	P	Hypothesis
H2a	PI <--- IG	0.431	0.057	7.577	***	Supported
H1a	AI <--- PI	0.573	0.046	12.582	***	Supported
H3a	SA <--- AI	0.406	0.043	9.346	***	Supported
H2b	SA <--- IG	0.139	0.042	3.296	***	Supported
H3b	QA <--- AI	0.15	0.048	3.115	0.002	Supported
H4	QA <--- SA	0.601	0.058	10.354	***	Supported
H1b	SA <--- PI	0.052	0.053	0.987	0.323	Not Supported
H2c	QA <--- IG	0.007	0.044	0.166	0.868	Not Supported
H1c	QA <--- PI	0.05	0.052	0.975	0.33	Not Supported

The AI construct (standardised path coefficient, β = 0.17, p < 0.001) and the SA construct (β = 0.56, p < 0.001) together were responsible for 44% of the QA (coefficient of determination, R^2 = 0.44). As a direct result, two hypotheses were validated: specifically, H3b and H4. The SA construct was estimated with the use of the AI (β = 0.49, p < 0.001) and IG constructs (β = 0.17, p < 0.001); this accounted for 31% of the SA construct (R^2 = 0.31). Accordingly, this finding aided in the validation of hypotheses H3a and H2b. In addition, the PI construct (β = 0.42, p < 0.001) was estimated with the use of the IG construct, which explained 18% of the PI construct (R^2 = 0.18), thereby supporting hypothesis H2a. Finally, the AI construct (β = 0.61, p < 0.001) was estimated using the PI construct, which was responsible for 37% of the AI construct (R^2 = 0.37), allowing hypothesis H1a to be supported. In contrast, H1b, H1c and H2c hypotheses were not supported by this research, and were therefore removed from the structural model.

4.6 CONCLUSION

In this chapter, SEM was used to validate the hypothesised, theoretical model of Active Situational awareness. The exploratory factor analysis reshaped the proposed model and broke down the intelligence into three component parts. This was deemed realistic because the variables grouping reflected three different types of intelligence, as explained in this chapter. Moreover, the perception, comprehension and projection that emerged in the hypothesised model came together into one construct, which reflects the Situational Awareness. In regard to Quality and Agility, the exploratory factor analysis merged them into one factor to create enhanced SA measured by quality and agility variables.

Active intelligence is the most significant construct to directly affect situational awareness and SA quality and agility, as this factor is considered to be the force multiplier that a defender should utilise when dealing with cyber attacks. Simply put: when cyber commanders rely on intelligence coming from an enemy domain, rather than from local sensors alone, then their SA will definitely be enhanced. The findings in this chapter show how important it is for the defender to interact with the enemy during cyber incidents in order to be able to identify an enemy's intention and motives behind the cyber attack, so that new knowledge can be gathered and cyber SA can be enhanced.

Both passive intelligence (PI) and intelligence gathering (IG) constructs are important to SA, as they both impact on SA and active intelligence. The reason is that active intelligence (AI) requires a direction in order to execute offensive attacks against an enemy; information that passive intelligence (PI) provides in the form of an enemy's IP address. Also, non-cyber intelligence is crucial in cyber SA, similar to the importance of resource availability, which is explained in terms of (IG) construct, as both impact intelligence and SA quality and agility.

To date, much has been discussed about the importance of SA in cyber security, but this the first time that a theory for active SA has been built that explicitly depicts the principal factors and their causal relationships as a structural equation model. Also, the model resulting from this chapter shaped the foundation for this research from which to develop and design techniques and methods for data collection, so that theory can be put into practice. The SEM model is used in this research to guide and inform the development of the serious gaming environment, SA BARS, and SA assessment metrics, as discussed in Chapter 3. Chapter 5 of this study will apply the causality model into the serious gaming environment in order to put the theory into practice through collecting data from participants using the above-mentioned instruments.

The results of the analysis revealed the importance of Active Offensive Intelligence gathering capability in enhancing cyber SA, which is predicted by measuring Situational Quality & Agility (QA). The SEM showed there is a significant impact on SA Agility and Quality from Active Intelligence gathering activities. Active defence is required for future cyber security. However, this trend towards the militarisation of cyberspace demands new or updated laws and regulations at an international level.

Active intelligence methods now determine the principal capability that must be at the core of new active situational awareness (aSA) models if they are to deliver enhanced agility and quality in cyber SA.

CHAPTER 5: SERIOUS GAMING TESTING ENVIRONMENT ASAM EXPERIMENT RESULTS

5.0 EXPERIMENT OVERVIEW

This chapter examines the results of the lab experiment conducted to test and verify the causal model derived from SEM, in order to see how active intelligence gathering enhances cyber SA agility and quality to deter cyber attacks. The experiment session was held between two controls. The first group was not exposed to an active environment, and participants dealt with cyber incidents using defensive techniques, whereas the second group were given access to the active component of a serious gaming environment more detail discussed earlier in chapter 3 and detail about the experiment is also attached in appendix 3. The following part of this study describes the analysis and findings of the experiment that used the causal model derived from SEM and put it in practice.

5.0.1 Participants

20 cyber security male experts taking from the original survey sample frame, with more than two years' experience apiece, participated in this study, as discussed in Chapter 3 section 3.2.The mean age was 25 (SD = 0.44). Of these 20 participants, ten were experts with a military background. The recruiting process for this experiment used the department's relations with cyber security firms.

5.0.2 Procedure

Participants were briefed about the experiment, as discussed in section 3.2.6.2 of Chapter 3. The researcher verbally and practically took participants through the experimental procedure in order to clarify the task at hand. In order to build familiarity with the serious gaming environment developed for the study, the researcher explained the system components in detail. This was achieved by including practical demonstrations, which also helped to highlight the functionalities of each tool in the system. Participants were given 15 minutes to acclimatise to the system and test its capabilities in real-time. In addition, during the initial briefing the researcher verbally explained how the data would be collected during the experiment, and explained to the participants how to use the data-gathering tool. The latter point aids the researcher to objectively measure participants' SA using a behavioural anchor rating scale. Finally, prior to the experimental phase, all participants were asked to fill out a questionnaire which contained demographic information.

5.0.3 Experiment execution

The Active SA theory was deployed in the experiment where different players have different roles. The Cyber Commander in the experiment was responsible to monitor the ADX system using the IDS (Snoby), Network monitoring tool (Capsa), System Log (SQL, Windows server 2008, Windows IIS server) in order to identify any suspicious activities in ADX system. Blue Team (one certified ethical hacker) as discussed earlier in chapter 3 section 3.2.6.2, was responsible to take offensive task orders

from cyber commander and provide the required intelligence. Cyber operators in the experiment were two people who assisted the cyber commander in monitoring the ADX system. Red team was another certified ethical hacker who has the role to launch the cyber attacks according to the experimental scenario using the script developed for this purpose. The data collecting instrument was filled by the cyber commanders during the experiment where timestamp was captured using the script that ask participant to answer the 4 main SA question as discussed in chapter 3 section 3.2.6.9. The researcher during the experiment was observing the participants performance and record their activities as participant were ask to speak loud during the exercise. The control group during the experiment had no access to the serious gaming environment active components (Deception and blue team) where cyber commanders were restricted with passive defence (Blocking).

After the experiment, the researcher went through participates SA results and observation notes in order to objectively mark them using SA BARS as discussed in chapter 3 section 3.2.6.10 which was developed in this research through exploiting the result of SEM and pilot it using subject matter experts in order to be able to identify the proper anchors and the standard operation procedures. Once the researcher completed the SA BARS, the result then fused into SA assessment metric (section 3.2.6.11) to measure the SA performance (efficiency, efficacy and effectiveness) which provided a quantifiable measures for Cyber SA. This chapter is going to discuss the analysis conducted for the result captures front the experiment.

5.0.4 Simulation and Experiment Network

Generation of realistic network traffic is crucial for any simulation environment. The serious gaming environment in this research achieved that by using different methods. First, the environment built with three networks as described in figure 3. In the internet, there were 7 legitimate users who accessed the experiment network assets during the experiment where normal traffic is generated. Also, some up-normal traffic such as failed log-in was generated when legitimate user from the Internet type in a wrong password. In addition, in this experiment, the attacker was generating malicious traffic when he/she conducted the cyber attack against ADX assets. Second, there were 7 local legitimate users within the LAN that were accessing the ADX resources and other resources in the internet. During the experiment, these local users accessed the ADX resources (web server, SQL server) and Internet (YouTube, Google, Sound cloud). Therefore, The IDS, Network monitoring and System log were getting load of information and that was enough to confuse the Cyber commander which is enough to represent a real case scenario.

5.0.5 Materials

As explained in the methodology chapter section 3.2.6.2.4, this study involved the design and development of a serious cyber-gaming, war-based environment based on the result found on the SEM analysis. In this study, participants were asked to act as cyber commanders. Their objective was to defend the serious gaming environment network assets using the available resources provided. A command and control centre was set up wherein participants were granted access to the latest

visualisation tools for both network and system monitoring. In addition, access was given to the network and system threat alert tools. During the control group (passive) exercise, the cyber commander had access to the IDS, firewall, system and network monitoring systems, and s/he was able to use these tools to try to detect any network threat and build situational awareness. On the other hand, the experimental group (active) was given access to the deception and offensive capabilities through the advance intelligence reporting system, which allowed sharing cyber intelligence with stakeholders and the blue team. In addition, for this experiment, this research designed and developed an assessments metrics and data capturing instruments in order to evaluate the performance of participants adapting active SA theory in practice and determine how active SA improves or enhances SA as discussed previously in section 3.2.6.2.5 of chapter 3 where quality and agility factor variables were used to develop the required metric which was piloted and validated by cyber security experts as discussed in chapter 3 section 3.2.6.2.5. In general, this informs what training, techniques and practices people need to go through to enhance their performance in future.

5.1 DATA PREPARATION

Section 3.2.6.2 of chapter 3 explained what instruments used for this analysis. Data were gathered from participants using an open-ended questionnaire and computerised tool was developed for this purpose to ensure data captured correctly and timely (appendix 3). Also, the performance of the participants and actions were recorded by researcher observation as participants were asked to speak loud while dealing with the environment. Later, this result were analysed to fill this research SA BARS which has been developed to understand how participant performed while dealing with the cyber scenario given as described in section 3.2.5 of chapter 3. Finally, the finding of the above instrument fused into SA measurement framework so cyber SA can be measured in quantitative manner. This process of gathering and generating result allowed this research to objectively mark participants as SA BARS was validated by SME's and SA measurement metrics were developed based on the cyber scenario where scores are either 0 and 1. Therefore, bias is not possible in this research. (Section 3.2.6.2.5)

5.1.1 Data Coding and Editing

In an attempt to ensure data consistency and comprehensiveness, this study carried out both editing and coding of the collected dataset after the researcher had objectively marked the performance of the participants using the instruments designed for this research. Missing or incomplete data were not taken into account, as this study analysed only complete datasets. In the event of any observable outliers, validation of why the outliers had surfaced was carefully inspected by re-examining the original questionnaire.

5.1.2 Data Screening

5.1.2.1 Normality test

A normality test was carried out in order to ensure that the data did not violate the normality assumption. The Jarque-Bera (skewness-kurtosis) test was applied to the data to ensure that they were within the acceptable limit of the skewness-kurtosis range (Hair et al., 2006). Skewness-kurtosis

critical values have been discussed and examined by many different academics (Hair et al., 2006; Tabachnick & Fidell, 2007), and were within the range of ± 2.58 at the 0.01 significance level. The skewness and kurtosis values of the constructs in this study were identified as being between the recommended critical values, confirming that the data were (univariably) normally distributed. Furthermore, for this study normal probability plots were performed for each construct alone. The findings highlighted no significant deviation from normality. Thus, results from the normal probability plots implied that data transformation was not essential (Tabachnick & Fidell, 2007).

5.1.2.2 Reliability test

Cronbach's alpha reliabilities for all of the constructs were above 0.943, thus surpassing the minimum value of 0.70 suggested by Field (2005).

5.2 ANALYSIS & RESULTS

The analysis involve comparing two groups (active and passive) where Data from SA BARS and SA assessment metric were used during the analysis to identify the differences in participants performance. Section 4.5.3 of chapter 4 verified the causality model of active SA theory, and the main aim of this research is to determine whether active SA enhance cyber SA and find out the degree of enhancement. Therefore, this section is going to discuss about the results found while applying the active SA theory and causality model into practice. This achieved in this research by conducting lab experiments using the serious gaming environment developed for this research as discussed in chapter 3 section 3.2.6.2.4. The following analyses are looking for differences between experiment group and control group, which look into how much cyber SA, enhance when active posture and active components utilised. Also, it will look into other issues such as how deception adoption impacts the cyber SA. Finally, the utilisation of blue team which in this research is the offensive capabilities that can be used to attack back the enemy and collect active intelligence from cyber enemy domain as discussed in section 3.2.6.2.4.4 of chapter 3.

5.2.1 Independent Sample T-Test

In this section, the analysis of passive and active conditions applied to the two independent groups revealed that there is a significance difference between the passive group and active group. The result of this analysis shows that there was a significant enhancement in cyber SA performance among experiment group (Active) and this supported by dramatic enhancement in participants cyber SA perception, comprehension and response by around 40%. The enhancement of overall cyber SA performance was around 35% where the active group significantly outperformed the passive group. Therefore, this confirms the research main question where active offensive intelligence gathering enhances cyber SA and this confirms that Active SA is a force multiplier that helped the active group to perform better than passive group.

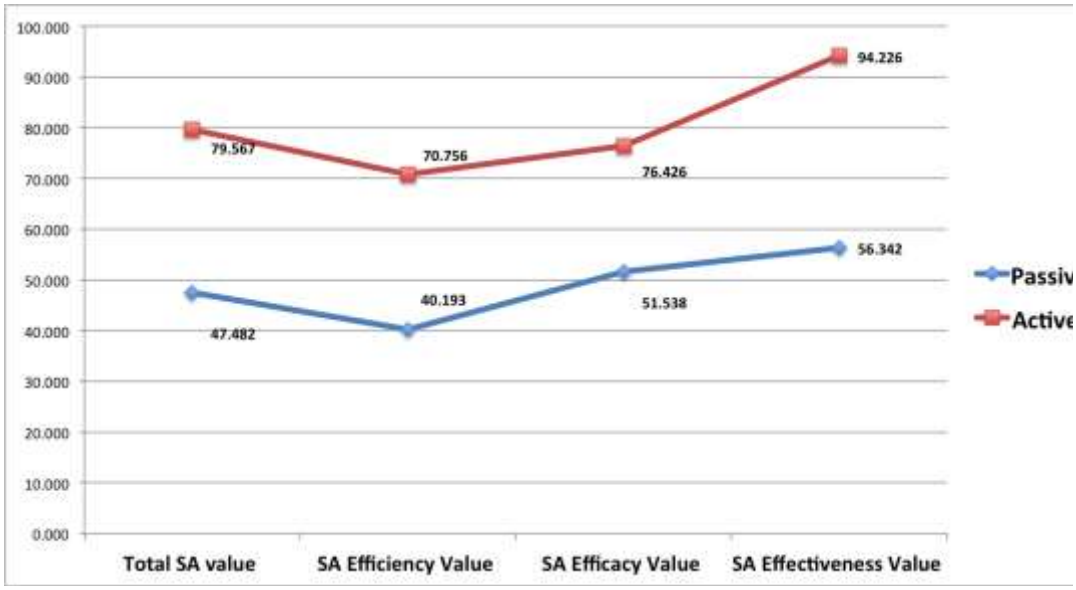
Another analysis conducted in this research was for military and non-military conditions to determine how education background impact in the performance of cyber SA using both active and passive group.

The results show that, a participant who comes from military background performed better than those who have civilian background. The military group in this analysis scored 25% more in overall cyber SA performance. The result also confirmed that military group had more tendency to apply offensive methods comparing with non-military who hesitated to adopt such service. This tells us that training and education is required for non-military organisations that might wish to adopt the active cyber SA.

a. Passive and Active conditions:

As describe earlier this test was performed using Data captured from SA BARS (Table 3.9) and Data calculated using SA assessment frameworks (Table 3.11). Therefore, an independent sample t-test was performed to see whether there were significant differences between the passive and active groups in the participants' perceptions of correctness and completeness, their analysis capabilities and also in their degree of comprehension and confidence. Independent sample t-tests were also used to assess whether any differences existed in the accuracy and timeliness of captured information, the timeliness of awareness building, the capability to act and respond, the capability to adapt to changes, the total SA, SA efficiency, SA efficacy, SA effectiveness and, finally, the overall participant SA and action in deterring cyber incidents in both Active and Passive intelligence gathering and defence conditions. The results showed significant differences in the scores for active and passive conditions (Figure 5.1, Table 5.1).

Figures 5.1: Means (Passive, Active) (Source: Author)



Figures 5.1.1: Means (Passive, Active) (Source: Author

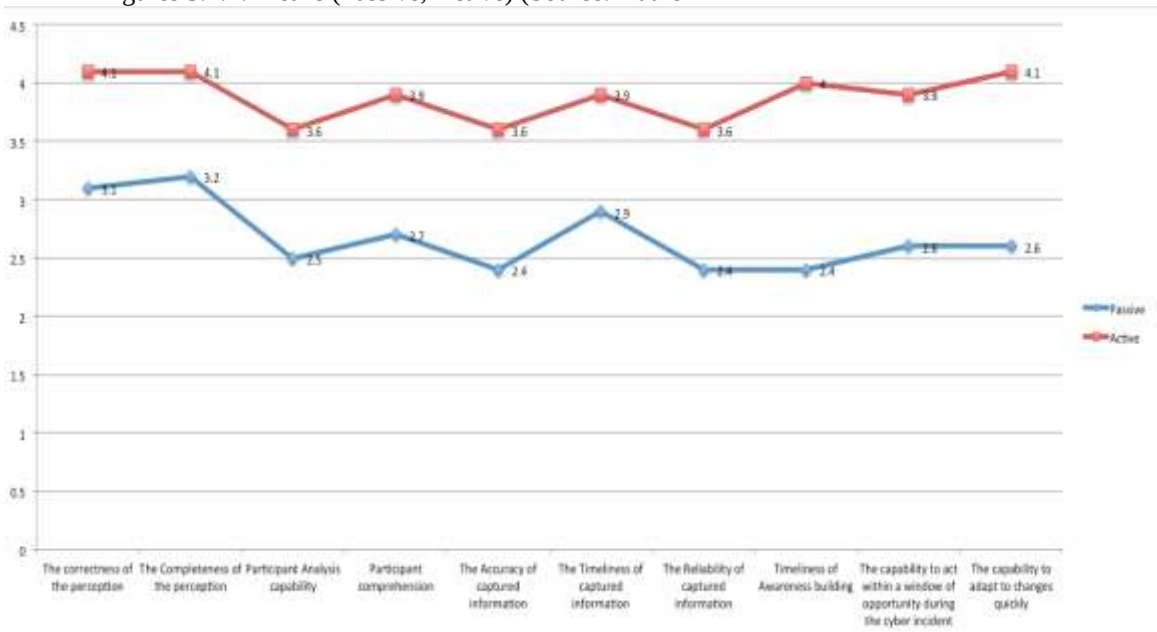


Table 5.1: Independent Sample T-Test (Passive, Active)

Independent Samples Test (Active, Passive)	T	df	Sig. (2-tailed)
The correctness of the perception	-2.249	18	0.037
The completeness of the perception	-2.102	18	0.05
Participant analysis capability	-2.283	18	0.035
Participant comprehension	-2.114	18	0.049
The accuracy of captured information	-2.959	18	0.008
The timeliness of captured information	-2.249	18	0.037
Timeliness of awareness building	-3.748	18	0.001
The capability to act	-2.672	18	0.016
The capability to adapt	-3.421	18	0.003
Total SA value %	-3.268	18	0.004
SA efficiency value %	-2.847	18	0.011
SA efficacy value %	-2.030	18	0.057
SA effectiveness value %	-3.588	18	0.002
Overall participant SA and action in deterring cyber incidents	3.286	18	0.004
The reliability of captured information	-2.959	18	0.008

Variables	Conditions (Means and SD)
Total SA value %	Passive (M=47.4821, SD=25.6144), Active (M=79.56705, SD=.17.547514)
SA efficiency value %	Passive (M= 47.4820, SD= 25.6143), Active (M= 79.57, SD= 17.55)
SA efficacy value %	Passive (M= 35.294, SD= 21.1), Active (M= 69.48, SD= 24.59)
SA effectiveness value %	Passive (M= 36.69, SD= 19.11), Active (M= 72.55248619, SD= 27.42)
The correctness of the perception	Passive (M=3.10, SD=1.10050), Active (M=4.100, SD=.8756)
The completeness of the perception	Passive (M=3.20, SD=1.03280), Active (M=4.100, SD=.87560)
Participant analysis capability	Passive (M=2.50, SD=1.17851), Active (M=3.60, SD=.96609)
Participant comprehension	Passive (M=2.70, SD=1.33749), Active (M=3.90, SD=1.19722)
The accuracy of captured information	Passive (M=2.40, SD=.84327), Active (M=3.60, SD=.96609)
The timeliness of captured information	Passive (M=2.9, SD=1.10050), Active (M=3.90, SD=.8756)
The reliability of captured information	Passive (M=2.40, SD=.84327), Active (M=3.60, SD=.96609)
Timeliness of awareness building	Passive (M=2.40, SD=.96609), Active (M=4, SD=.94281)
The capability to act	Passive (M=2.6, SD=1.26491), Active (M=3.90, SD=.8756)
The capability to adapt	Passive (M=2.6, SD=1.17379), Active (M=4.10, SD=.73786)
Overall participant SA	Passive (M=1.70, SD=.48305), Active (M=1.10, SD=.31623)

Table 5.1.1: Means and SD (Passive, Active)

With respect to table 5.1-5.1.1 and figure 5.1-5.1.1, the results from the participants' total SA [t(18)=-3.268, p= 0.004], SA Efficiency [t(18)=- 2.847, p= 0.011], SA Efficacy [t(18)= 2.030, p= 0.05] and finally SA Effectiveness [t(18)= 3.588, p=0.002] highlight a significant effect on and improvement in active group's SA. Overall the active group in the serious gaming experiment scored higher than the passive control group. This is due to enhancements of the participants' SA building process; specifically, the Behaviour Anchor Rating (BAR) revealed that participants' perception correctness [t(18)=-2.249, p= 0.037] and completeness [t(18)=-2.102, p= 0.050] were both markedly improved during the active session, as participants were alerted to a sufficient amount of data/intelligence to enable them to prevent the potential cyber incident i.e. the cyber threat..

Another possibility to explain the improvement in the participants' SA was the effect of their analysis capabilities [t(18)=-2.283, p= 0.035], comprehension and confidence [t(18)=-2.114, p= 0.049]. The results reveal that these were significant effects, and also suggest that the Active offensive defence group managed to understand the situation with greater confidence than the Passive group, where the latter hesitated to take action during the experiment. Also, this confirms the fact that the active group had a force multiplier shaped in offensive capabilities that allowed participants to generate more intelligence which eventually enhanced their understanding regarding the given scenario.

The accuracy of captured information [t(18)=-2.959, p= 0.008] revealed one significant effect by which Active offensive defence aided the enhancement of the accuracy of information gathered about cyber incidents. In addition, the results of the timeliness of captured information [t(18)=-2.249, p= 0.037] demonstrate the greater effectiveness of Active offensive defence in capturing incident information. The reliability of the garnered information [t(18)=-2.959, p= 0.008] showed that there was a significant effect whereby Active offensive defence aided the enhancement of the reliability of information gathered about cyber incidents. These results were reflected in the test for Timeliness of Awareness building [t(18)=-3.748, p= 0.001], which revealed a significant consequence of building situational

awareness in a timely manner: Active defence was significantly faster and stronger in SA building as a result. Consequently, the capability to both act and respond [t(18)=-2.672, p= 0.016], and the participants' capability to adapt to changes [t(18)=-3.421, p= 0.003], were significantly improved during the active sessions in which the group that employed Active offensive defence capabilities scored higher, as compared to the passive control group, thus, showing the importance of active defence in cyber security.

Finally, the results from overall Participant SA and action in deterring cyber incidents [t(18)=3.286, p= 0.005] is a significant effect and confirmed the importance of adopting a winning attitude; i.e. utilising an offensive method to defend cyberspace is better than adopting the traditional view of passive defence.

a.1 Effect Size:

In order to determine the effect size between active and passive group, Cohen's d effect size for t-test was adopted using the following formula for the total SA performance:

$$d = \frac{|\bar{X}_1 + \bar{X}_2|}{\sqrt{\frac{(\sigma_1^2 + \sigma_2^2)}{2}}} = \frac{|47.482 + 79.567|}{\sqrt{\frac{(25.614_1^2 + 17.547_2^2)}{2}}} = 1.46145126$$

Where x1 and x2 are the means of group 1 and group 2, and σ12 and σ22 are the variances of group 1 and group 2. The result of the effect is greater than .8, which reveals there is a large effect. (Cohen, 1988).

b. Military and non-military conditions:

Independent sample t-tests were conducted to compare the military and non-military groups to determine whether there were differences in participants' perception correctness and completeness, analysis capabilities, comprehension levels and self-confidence. T-tests were also performed to assess whether there were any significant differences in the accuracy and timeliness of captured information, the timeliness of awareness building, the capability to act, respond to and to adapt to changes, and the total SA in a participant's background (military/non-military) conditions. As this research previously established, the attitude to cyber defence should be changed from preventive, passive defence to a winning attitude: one that seeks to use offensive countermeasures against cyber attack. The results highlight a significant difference in the scores between military and non-military conditions in favour of the military group (Table 5.2, 5.2.1, Figure 5.2, 5.2.1).

Figure 5.2: Means (military, non-military)

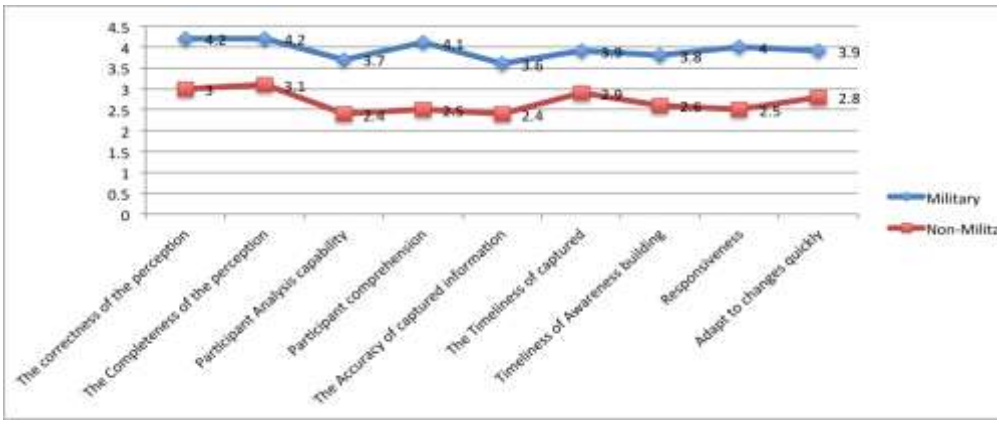


Figure 5.2.1: Means (military, non-military)

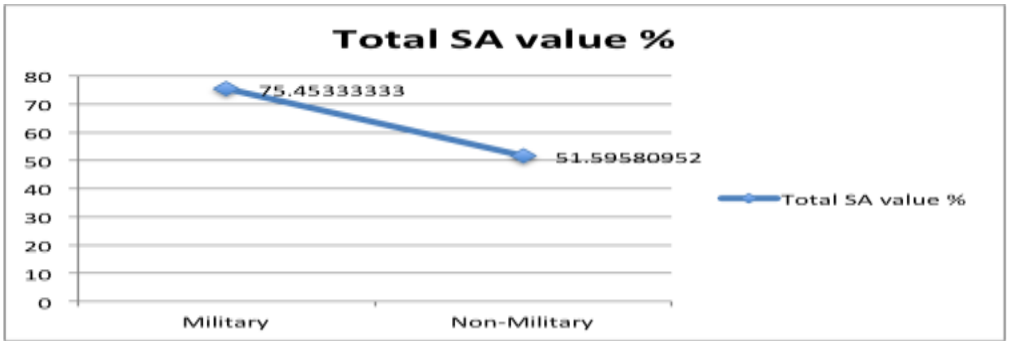


Table 5.2: Independent Sample T-Test (military, non-military)

Independent Samples Test (Military, Non Military)	T	df	Sig. (2-tailed)
The correctness of the perception	2.882	18	0.01
The completeness of the perception	2.741	18	0.013
Participant analysis capability	2.867	18	0.01
Participant comprehension	3.138	18	0.006
The accuracy of captured information	2.959	18	0.008
The timeliness of captured information	2.249	18	0.037
Timeliness of awareness building	2.427	18	0.026
The capability to act	3.308	18	0.004
The capability to adapt	2.2	18	0.041
Total SA value %	2.16	18	0.044

Variables	Conditions (Means and SD)
Total SA value %	Military (M=75.453, SD=18.938), non-military (M=51.59, SD=29.34384)
The correctness of the perception	Military (M=4.20, SD=.63246), non-military (M=3, SD=1.1547)
The completeness of the perception	Military (M=4.20, SD=. 63246), non-military (M=3.100, SD=1.1005)
Participant analysis capability	Military (M=3.70, SD=.82327), non-military (M=2.40, SD=1.17379)
Participant comprehension	Military (M=4.10, SD=.56765), non-military (M=2.50, SD=1.50923)
The accuracy of captured information	Military (M=3.60, SD=1.07497), non-military (M=2.40, SD=.69921)
The timeliness of captured information	Military (M=3.90, SD=1.10050), non-military (M=2.90, SD=.8756)
Timeliness of awareness building	Military (M=3.80, SD=1.22927), non-military (M=2.60, SD=.96609)
The capability to act	Military (M=4, SD=.81650), non-military (M=2.50, SD=1.17851)
The capability to adapt	Military (M=3.9, SD=1.19722), non-military (M=2.80, SD=1.03280)

Table 5.2.1: Means And SD (military, non-military)

With respect to table 5.2-5.2.1 and figure 5.2-5.2.1, the results from the participants' perception correctness [t(18)=2.882, p= 0.010], and participants' perception completeness [t(18)=2.741, p= 0.013] demonstrate a significant effect on participant perception correctness and completeness. This implies that those who had a military background and a military way of thinking scored higher than those with a non-military background. With regards to participant analysis capabilities [t(18)=2.867, p= 0.010] and participant comprehension and confidence [t(18)=3.138, p= 0.006], the results show a significant effect on a participant's ability to understand the situation. The findings from the accuracy of captured information [t(18)=2.959, p= 0.008], the timeliness of captured information [t(18)=2.249, p= 0.037], and the timeliness of awareness building [t(18)=2.427, p= 0.026] indicate that there were significant effects on a participant's performance with regards to both information capturing and predicting future incidents. In addition, a participant's capability to act and respond [t(18)=3.308, p= 0.004], and their capability to adapt to changes [t(18)=2.200, p= 0.041] could be compared; the results of these comparisons reveal significant differences, suggesting that those participants who had a military background were significantly better in responding to cyber incidents. Finally, results obtained from participants' total SA [t(18)=2.160, p= 0.044] reveal the significant effect of participants' backgrounds on their total SA. The findings overall support the argument of this research outlined earlier: that a winning attitude, i.e. using offensive countermeasures enhances a commander's situational awareness.

5.2.2 One-Way ANOVA

In this section one-way ANOVA analysis was performed to determine how deception and blue team with offensive capabilities impact cyber SA performance. With respect to blue team utilisation, the results confirm that there was a significant effect in participant cyber SA performance which reveal that participants who utilised offensive active capabilities during the experiment scored better in overall cyber SA performance and managed to deter cyber attack in an efficient and effective way compare to those who either failed to utilise or decided to use passive features of the blue team. This result also confirms that training and practice is required in order to be able to gain full advantages of active cyber SA.

The second analysis in this section was to determine how deception impacts participant's performance during the experiment. The result in this analysis revealed that participant's who utilised deception

service correctly performed better other who failed to utilise this service. The results also show that there was around 40% enhancement in participant's cyber SA performance when deception was used correctly. However, the results confirm that when deception is not used correctly due to false positive issue, participants' cyber SA dropped dramatically which shows that deception capability is a double edge sword so it should be utilised carefully. Also, this confirms training is necessary for participants to learn how to use deception to avoid making mistakes in future.

a. Utilisation of the blue team capability conditions:

In this analysis a one-way ANOVA (**Dependent:** Total SA, SA efficiency, efficacy and effectiveness, **Independent:** blue team utilisation conditions) was performed in order to compare the effect of utilising the blue team (Grouped based on SA BARS) with offensive capability among participant to determine whether there were a significance differences in participants total SA, SA efficiency, SA efficacy and finally SA effectiveness. Further, a one-way ANOVA was used to determine whether any significant differences existed between the way participants utilised blue team capabilities: specifically, comparing the effect of blue team utilisation conditions on each participant's perception correctness, perception completeness, analysis capabilities and comprehension and confidence, as well as the accuracy of captured information, the timeliness of captured information, the timeliness of awareness building, the participant's capability to act and respond, and finally his/her capability to adapt to changes. The analysis (Table 5.3) revealed that there was a significant effect of arming the blue team with offensive capability on total SA, SA efficiency, SA efficacy and SA effectiveness at the $P<0.05$ level for the way participants utilise blue team capability conditions [Total SA $F(2,17)=10.179$, $P = 0.001$], [SA Efficiency $F(2,17)=14.263$, $P = 0.000$],[SA Efficacy $F(2,17)=14.607$, $P = 0.000$], [SA Effectiveness $F(2,17)=10.777$, $P = 0.001$]. The results also indicated that there were significant effects on participants' perception correctness [$F(2,17)=6.573$, $P = 0.008$], perception completeness [$F(2,17)=6.345$, $P = 0.009$], analysis capabilities [$F(2,17)=7.362$, $P = 0.005$] and [$F(2,17)=6.345$, $P = 0.009$], the accuracy of captured information [$F(2,17)=14.140$, $P = 0.000$], timeliness of captured information [$F(2,17)=7.012$, $P = 0.006$], timeliness of awareness building [$F(2,17)=15.036$, $P = 0.000$], and the participant's capability to act and respond [$F(2,17)=7.726$, $P = 0.004$] and adapt to changes [$F(2,17)=8.184$, $P = 0.003$] under these conditions. Interestingly, these results highlight the fact that participants' total SA, SA efficiency, SA efficacy, SA effectiveness, participant's perception correctness, participant's perception completeness, participant's analysis capabilities, participant's comprehension and confidence, accuracy of captured information, timeliness of captured information, timeliness of awareness building, capability to act and respond, and the capability to adapt to changes were dramatically enhanced as their performance as a consequence of utilising active blue team capability for deterring cyber attacks.

Table 5.3: One-Way ANOVA (blue team utilisation conditions)

ANOVA						
		Sum of Squares	df	Mean Square	F	Sig.
The correctness of the perception	Between groups	9.943	2	4.971	6.573	0.008
	Within groups	12.857	17	0.756		
	Total	22.8	19			
The completeness of the perception	Between groups	8.784	2	4.392	6.345	0.009
	Within groups	11.766	17	0.692		
	Total	20.55	19			
Participant analysis capability	Between groups	12.508	2	6.254	7.362	0.005
	Within groups	14.442	17	0.85		
	Total	26.95	19			
Participant comprehension	Between groups	15.473	2	7.736	6.345	0.009
	Within groups	20.727	17	1.219		
	Total	36.2	19			
The accuracy of captured information	Between groups	13.74	2	6.87	14.14	0.000
	Within groups	8.26	17	0.486		
	Total	22	19			
The timeliness of captured information	Between groups	10.306	2	5.153	7.012	0.006
	Within groups	12.494	17	0.735		
	Total	22.8	19			
The reliability of captured information	Between groups	13.74	2	6.87	14.14	0.00
	Within groups	8.26	17	0.486		
	Total	22	19			
Timeliness of awareness building	Between groups	18.655	2	9.327	15.036	0.000
	Within groups	10.545	17	0.62		
	Total	29.2	19			
The capability to act within a window of opportunity during a cyber incident	Between groups	14.166	2	7.083	7.726	0.004
	Within groups	15.584	17	0.917		
	Total	29.75	19			
The capability to adapt to changes quickly	Between groups	14.005	2	7.002	8.184	0.003
	Within groups	14.545	17	0.856		
	Total	28.55	19			
Total SA value %	Between groups	7532.959	2	3766.48	10.179	0.001
	Within groups	6290.356	17	370.021		
	Total	13823.315	19			
SA efficiency value %	Between groups	9560.262	2	4780.131	14.263	0.000
	Within groups	5697.273	17	335.134		
	Total	15257.535	19			
SA efficacy value %	Between groups	10419.056	2	5209.528	14.607	0.000
	Within groups	6063.124	17	356.654		
	Total	16482.179	19			
SA effectiveness value %	Between groups	9751.037	2	4875.518	10.777	0.001
	Within groups	7690.522	17	452.384		
	Total	17441.559	19			
Overall participant SA and action in deterring cyber incidents	Between groups	2.618	2	1.309	10.2	0.001
	Within groups	2.182	17	0.128		
	Total	4.8	19			

The effect of the blue team provided with offensive capability on the overall participant SA and on the action in deterring cyber incidents was conducted using a one-way ANOVA to determine whether there were any significant differences with how participants utilised blue team capability conditions. The analysis indicates that there was a significant effect of blue team utilisation on the overall participants' SA and action in deterring cyber incidents at the $P<0.05$ level [$F(2,17)=10.20$, $P = 0.001$].

Figure 5.3: Blue Team Utilisation Conditions and Situational Awareness

Figure 5.3.A: SA Effectiveness:

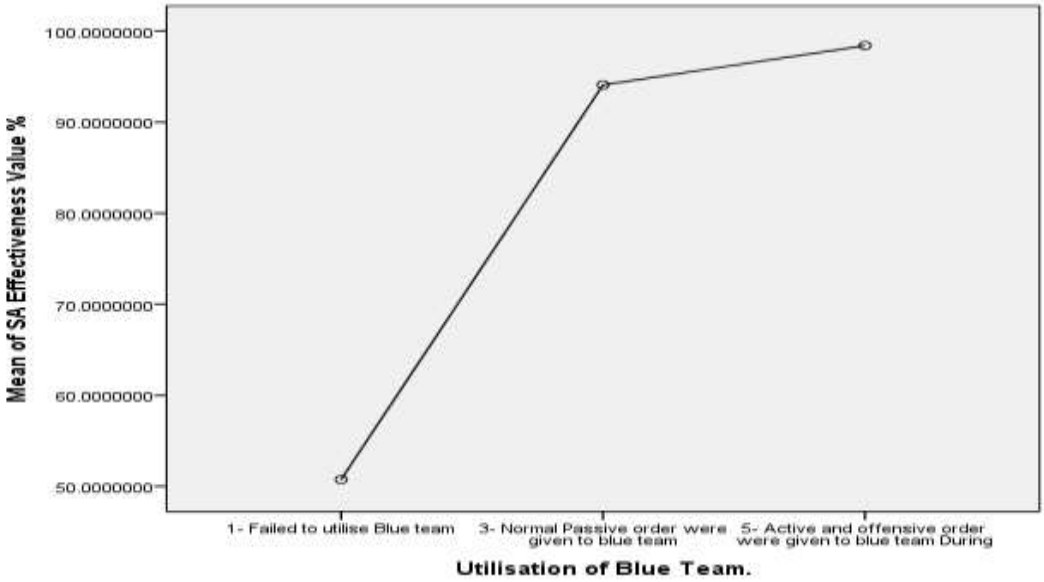


Figure 5.3.B: SA Efficacy:

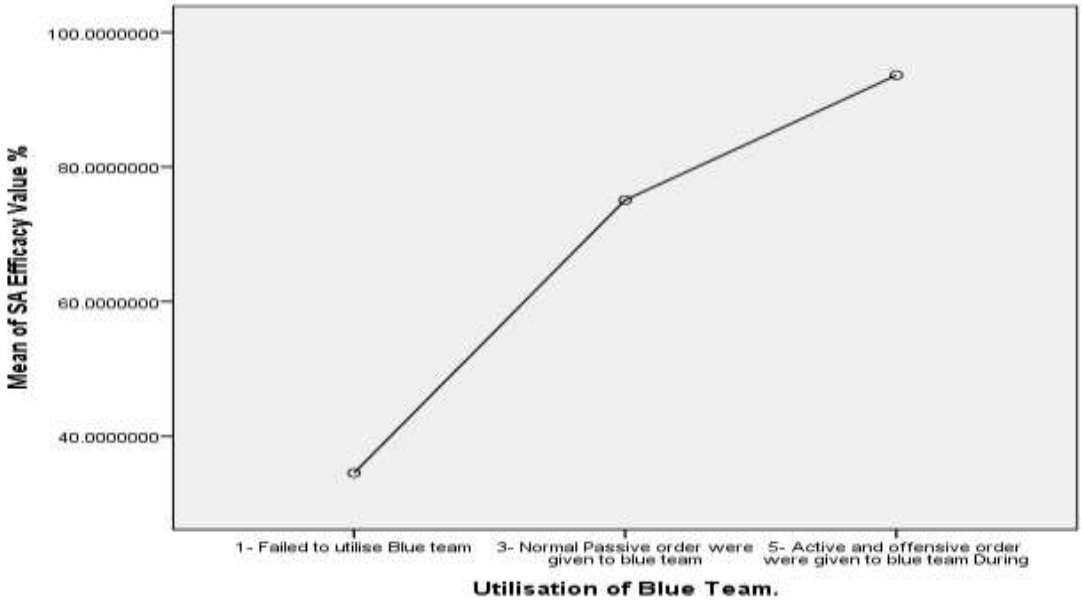


Figure 5.3.C: SA Efficiency:

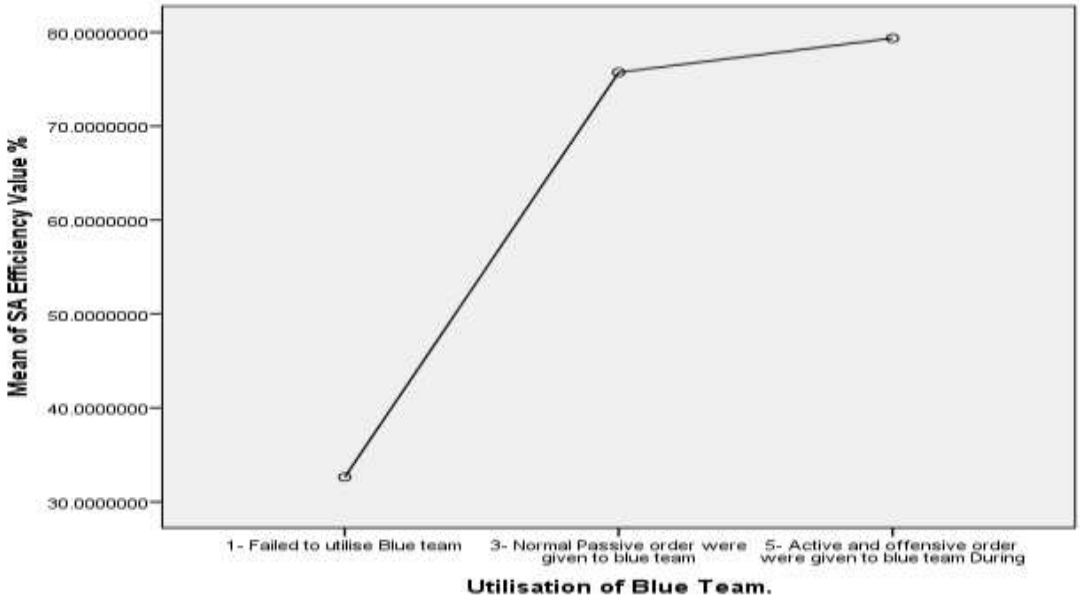


Figure 5.3.D: Total SA:

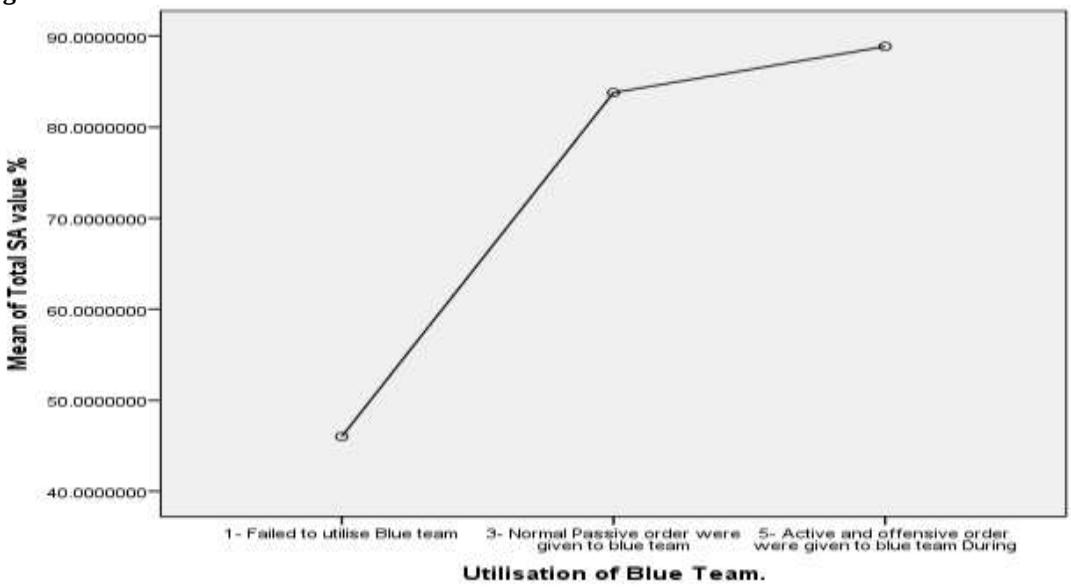


Figure 5.3.E: SA Overall:

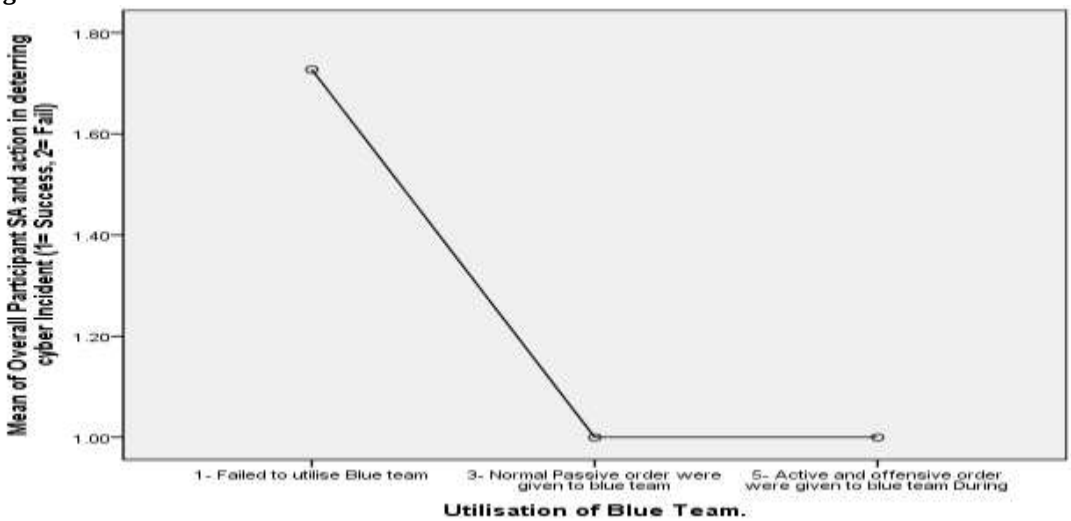


Figure (5.3 A,B,C,D,E) shows that participants who utilised offensive, or active, defence, were more likely to deter cyber incidents from occurring, and demonstrated overall more correct and strong SA as compared with participants who did not employ this method. This result supports the proposed research proposition that using offensive countermeasures in cyber defence is effective, as it helps prove that this method is a robust way for acting in such a complex domain. In addition, it was clear from the figures that those who utilised blue team's capabilities scored highly with regards to situational awareness, SA efficiency, SA efficacy and SA effectiveness; overall, participants' SA and actions during cyber incidents were significantly enhanced.

b. Utilisation of the deception conditions:

The effect of deception on participants' SA, SA efficiency, SA efficacy, SA effectiveness, perception correctness, perception completeness, analysis capabilities and participants' comprehension and confidence, and on the accuracy and reliability of captured information, the timeliness of captured information, the timeliness of awareness building, participants' capability to act and respond ability to adapt to changes were tested using a one-way ANOVA in order to determine whether significant differences existed between the way participants utilised cyber deception capability conditions. The results confirm that there was a significant effect of deception on total SA, SA efficiency, SA efficacy and SA effectiveness at the $P<0.05$ level for the way participants utilised cyber deception capability conditions [Total SA $F(3,16)=6.86$, $P = 0.003$], [SA Efficiency $F(3,16)=11.18$, $P = 0.000$], [SA Efficacy $F(3,16)=9.886$, $P = 0.001$], [SA Effectiveness $F(3,16)=7.284$, $P = 0.003$]. The results also indicate that there was a significant effect of deception on participants' perception correctness [$F(3,16)=4.130$, $P = 0.024$], perception completeness [$F(3,16)=4.156$, $P = 0.023$], analysis capabilities [$F(3,16)=3.622$, $P = 0.036$], and comprehension and confidence [$F(3,16)=4.670$, $P = 0.016$], and on the accuracy of captured information [$F(3,16)=4.959$, $P = 0.013$], timeliness of captured information [$F(3,16)=3.543$, $P = 0.039$], reliability of captured information [$F(3,16)=4.959$, $P = 0.013$] and timeliness of awareness building [$F(3,16)=8.092$, $P = 0.002$], and on participants' capability to act and respond [$F(3,16)=3.891$, $P = 0.029$] and adapt to changes [$F(3,16)=4.427$, $P = 0.019$] at the $P<0.05$ level when utilising deception capability conditions. Determining the effect of deception on participants' overall SA and actions in deterring cyber incidents was conducted using a one-way ANOVA (**Dependent:** Total SA, SA efficiency, efficacy and effectiveness, **Independent:** utilisation of deception).

Table 5.4: One-Way ANOVA (Deception utilisation conditions):

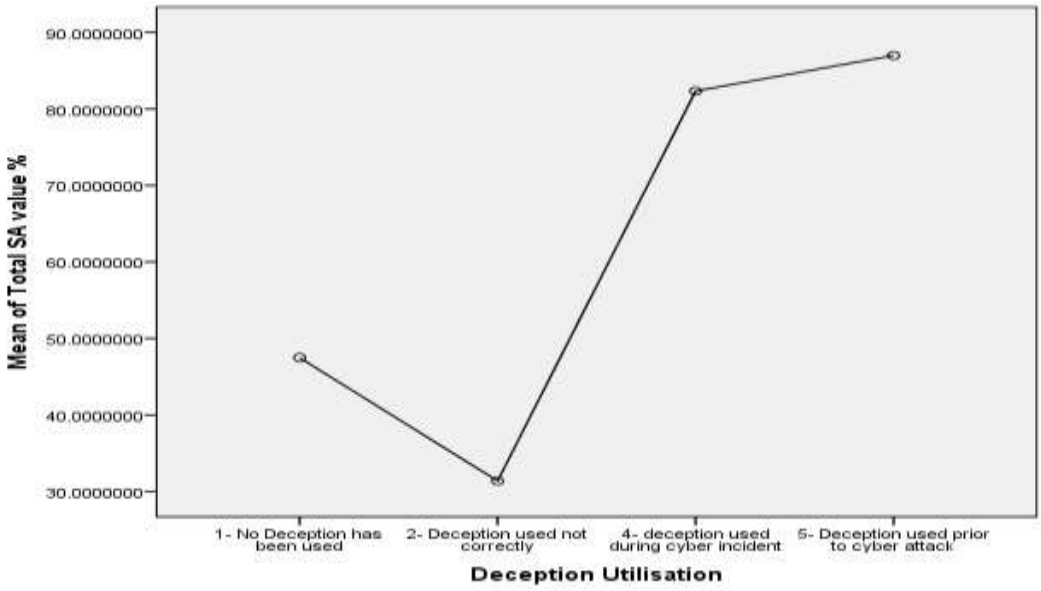
ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
The correctness of the perception	Between groups	9.95	3	3.317	4.13	0.024
	Within groups	12.85	16	0.803		
	Total	22.8	19			
The completeness of the perception	Between groups	9	3	3	4.156	0.023
	Within groups	11.55	16	0.722		
	Total	20.55	19			
Participant analysis capability	Between groups	10.9	3	3.633	3.622	0.036
	Within groups	16.05	16	1.003		
	Total	26.95	19			
Participant comprehension	Between groups	16.9	3	5.633	4.67	0.016
	Within groups	19.3	16	1.206		
	Total	36.2	19			
The accuracy of captured information	Between groups	10.6	3	3.533	4.959	0.013
	Within groups	11.4	16	0.713		
	Total	22	19			
The timeliness of captured information	Between groups	9.1	3	3.033	3.543	0.039
	Within groups	13.7	16	0.856		
	Total	22.8	19			
The reliability of captured information	Between groups	10.6	3	3.533	4.959	0.013
	Within groups	11.4	16	0.713		
	Total	22	19			
Timeliness of awareness building	Between groups	17.6	3	5.867	8.092	0.002
	Within groups	11.6	16	0.725		
	Total	29.2	19			
The capability to act within a window of opportunity during a cyber incident	Between groups	12.55	3	4.183	3.891	0.029
	Within groups	17.2	16	1.075		
	Total	29.75	19			
The capability to adapt to changes quickly	Between groups	12.95	3	4.317	4.427	0.019
	Within groups	15.6	16	0.975		
	Total	28.55	19			
Total SA value %	Between groups	7776.999	3	2592.333	6.86	0.003
	Within groups	6046.316	16	377.895		
	Total	13823.315	19			
SA Efficiency Value %	Between groups	10329.8	3	3443.267	11.18	0.000
	Within groups	4927.734	16	307.983		
	Total	15257.535	19			
SA Efficacy Value %	Between groups	10706.258	3	3568.753	9.886	0.001
	Within groups	5775.921	16	360.995		
	Total	16482.179	19			
SA Effectiveness Value %	Between groups	10069.178	3	3356.393	7.284	0.003
	Within groups	7372.381	16	460.774		
	Total	17441.559	19			
Overall participant SA and action in deterring cyber incidents	Between groups	2.7	3	0.9	6.857	0.004
	Within groups	2.1	16	0.131		
	Total	4.8	19			

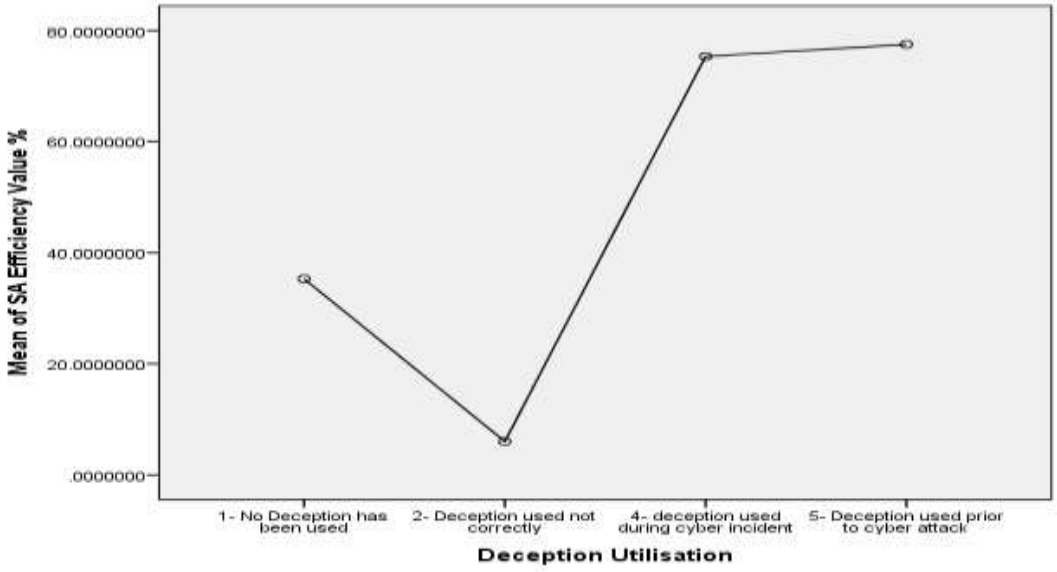
Moreover, the analysis indicates that there was a significant effect from the way participants utilised deception capability conditions on participants' overall SA and the action they took to deter cyber incidents at the $P<0.05$ level [$F(3,16)=6.857$, $P = 0.004$]. This finding revealed that participants' overall SA was enhanced when deception was utilised to deter cyber incidents.

Figures 5.4: Deception Utilisation Conditions and Situational Awareness:

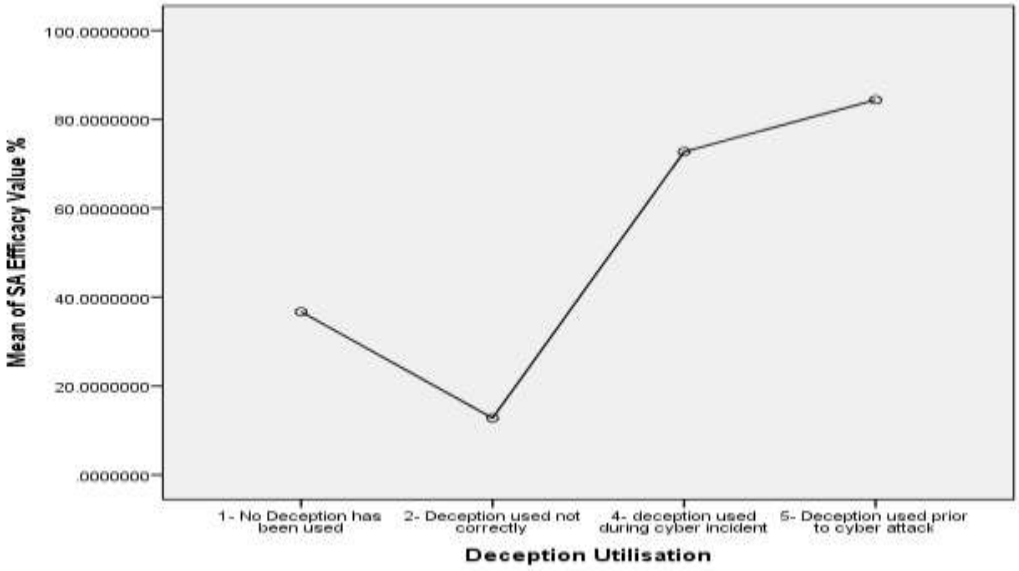
Figures 5.4.A: Total SA



Figures 5.4.B: SA Efficiency



Figures 5.4.C: SA Efficacy



Figures 5.4.D: SA Overall

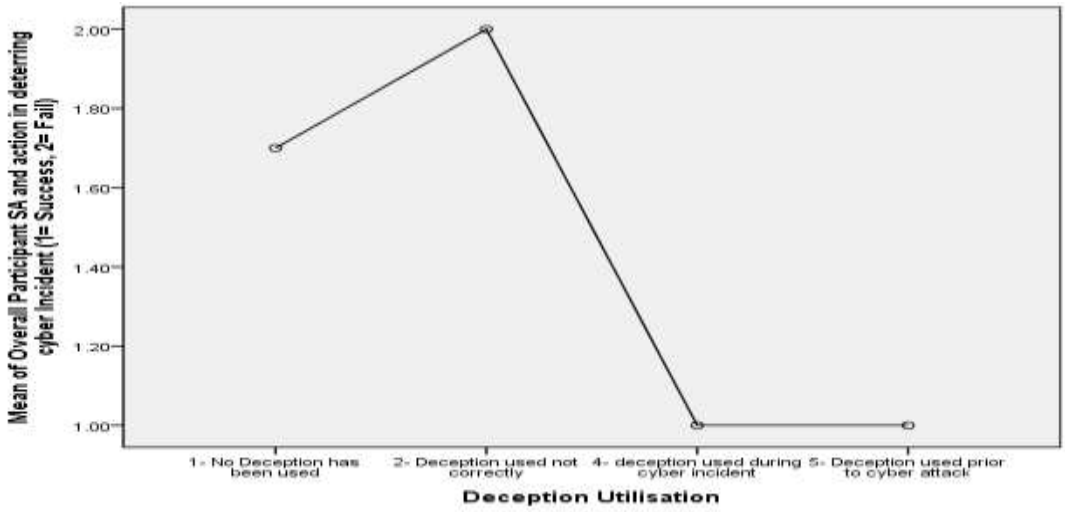


Figure (5.4 A,B,C,D) demonstrates that participants who utilised cyber deception managed to deter cyber incidents, and also exhibited correct and strong SA scores compared with participants who did not use it. Figure (5.4.A-D) reveals the importance of cyber deception in cyber security and active defence; the statistics show how participants' SA, SA efficiency, SA efficacy, SA effectiveness and overall SA and action were all significantly improved by utilising deception methods. However, Figure (5.4.A-D) demonstrates a significant negative relationship with regards to participant performance and incorrectly applied deception which represent the false positive where a participant anticipate legitimate traffic to be malicious. Thus, deception capability is a double-edged sword, and it should be used carefully in order to take full advantage of its capability.

5.3 RESULT DISCUSSIONS

The main purpose of this experiment in the research study was to validate the research hypothesis and answer the main research question by examining the role of active intelligence gathering using offensive hacking techniques to enhance cyber situational awareness agility and quality in dealing with cyber incidents. The results of the experiment, as described above, brought to light that participant situational awareness was significantly improved when a winning attitude (active offensive defence) was introduced. The independent sample t-test for active and passive conditions revealed that the participants' total SA mean (M) (Figure 5.5-7) (Table 5.1 & 5.1.1 Figure 5.1 & 5.1.1) improved by 32% where participants with a winning attitude scored a higher SA than the control group. In addition, participants' SA efficiency, efficacy and effectiveness were all enhanced by 35%. Moreover, the analysis revealed that participants' SA perception, comprehension and capability to project and deter cyber incidents were significantly improved in the experimental group; this eventually led to an enhancement of participants' agility and quality in dealing with cyber incidents. This finding confirms that active intelligence gathering, in combination with offensive hacking, enhances situational awareness agility and quality, thus verifying our hypothesis.

The second independent sample t-test (Table 5.2 & 5.2.1, Figure 5.2 & 5.2.1), performed on participants' backgrounds (military or non-military), was used to explore the impact of 'the military way of thinking' in using active defence and dealing with cyber incidents. The results of this test show that those who had a military way of thinking managed to deter cyber incidents significantly better; the mean of participants' total SA difference was 24% better than those who came from a non-military background. In addition, their situational awareness performance was significantly better, and helped them become more agile in preventing cyber incidents. This was because of their willingness to utilise both offensive methods and their skills in hacking.

Figure 5.5: Active Mean (Total SA, SA Efficiency, SA Efficacy, SA Effectiveness)

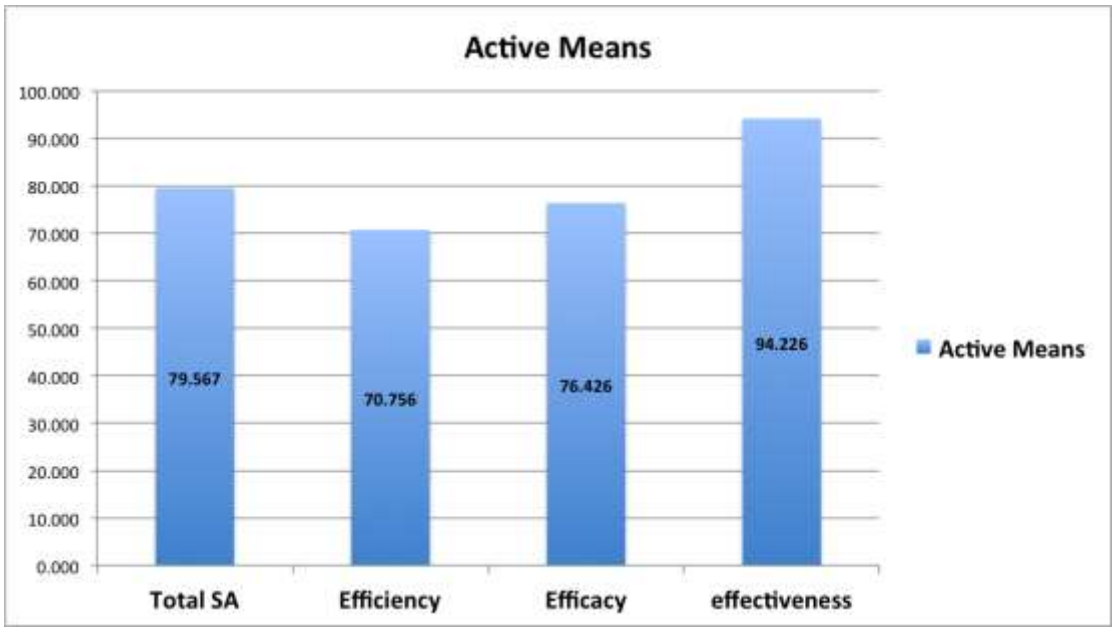


Figure 5.6: Passive Mean (Total SA, SA Efficiency, SA Efficacy, SA Effectiveness)

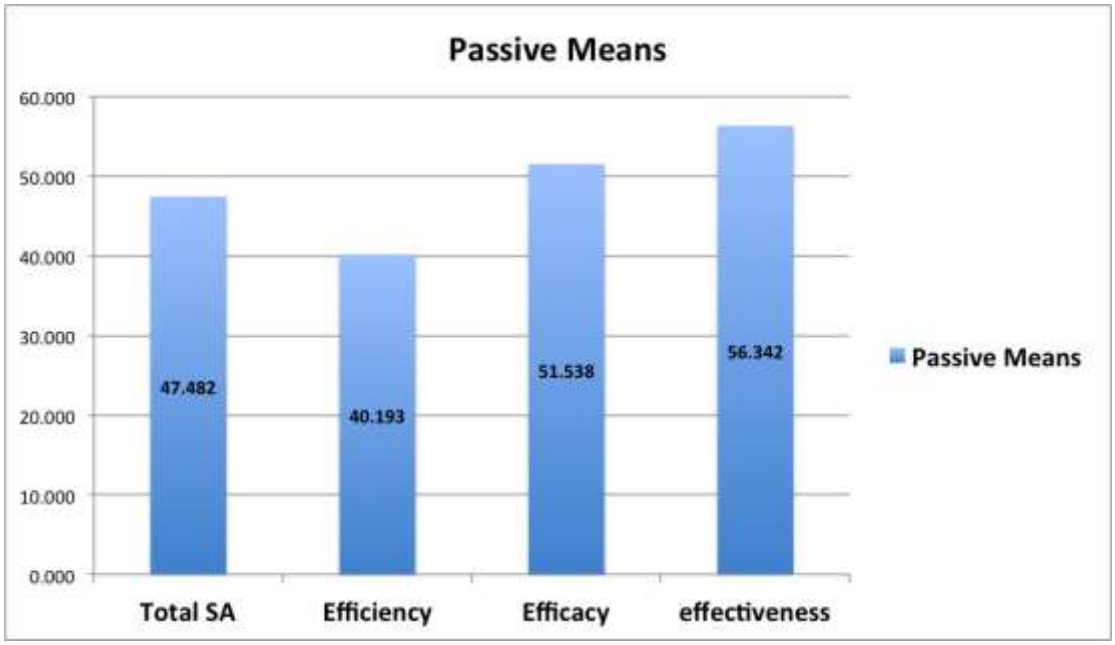
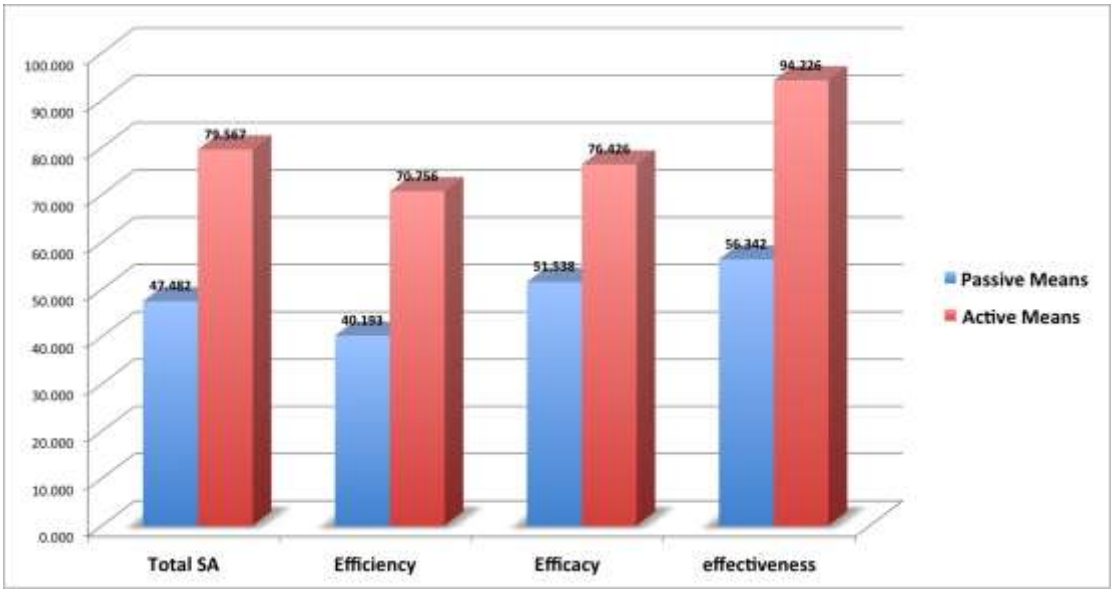


Figure 5.7: Passive Mean vs. Active Mean (Total SA, SA Efficiency, SA Efficacy, SA Effectiveness)



An additional test was conducted in this study: a one-way ANOVA was used to examine the impact of blue team's use of offensive capabilities and deception. The results (Table 5.3) (Figure 5.3.A-E) demonstrate that the participants' overall SA was significantly improved, suggesting that participants' SA performance was achieved in a high quality and agile manner as compared to the control group. Therefore, blue team's performance with offensive capabilities had a major impact on SA performance, and so it is a main factor that should be considered when active defence is adopted. With regards to the utilisation of deception, the analysis (Table 5.4.A-D) indicates that participants who utilised the deception service correctly performed significantly better than those who did not, or than those that used deception incorrectly, when it comes to SA performance. The analysis also helped to articulate the fact that deception services were used by participants to buy extra time, enabling them to better understand cyber incidents and so control the impact of these incidents more effectively. This highlighted the importance of deception in active cyber defence as a tool that enables cyber commanders to defend their network. However, the results (Figure 5.4.A-D) also reveal that incorrectly (false positive) utilising cyber deception resulted in participants failing to control cyber incidents, and their SA performance was poor in comparison to those who utilised it correctly. This shows how important strong cyber deception capability is in an active defence situation, but also demonstrates its limitations. In summary, deception capability is a double-edged sword, and it should be used carefully in order to take the full advantage of its capabilities. Cyber commanders should utilise it when convinced of the existence of suspicious network activities.

5.4 CONCLUSION

First and foremost, it was of critical to determine whether any significant differences existed between active and passive intelligence gathering and defence conditions. For this, the participants' perception of correctness and completeness, their analysis capabilities, comprehension and confidence, the accuracy and timeliness of the captured information, the timeliness of awareness building, their capability to act and respond and adapt to changes, the total SA, SA efficiency, SA efficacy and SA effectiveness, and the overall participant SA and action in deterring cyber incidents, were examined under prescribed simulation conditions. It became evident that, overall, during the active sessions participants perceived a sufficient amount of data, enabling them to deter cyber incidents more effectively than during passive sessions. Interestingly, further probing revealed that the active, offensive defence group managed to understand the situation at hand with more confidence, as compared with the passive group, where the latter showed hesitation in decision making. In addition, active offensive defence enhanced the accuracy of information gathered about cyber incidents, and the results also suggested that this strategy may well have been more effective for capturing incident-related information; this highlights the importance of active defence in cyber security. The results also provide evidence demonstrating the importance of adopting a winning attitude (utilising offensive methods) rather than passive defence methods, to effectively defend cyberspace.

The findings presented here also show that adopting a winning attitude is of importance with regards to the enhancement of a person's situational awareness. This conclusion is connected more to participants who had a military background than those without one. In fact, participants who had a military background were also found to be statistically better in responding to cyber incidents. Overall, the results shown in this chapter help to demonstrate that participants who utilised offensive, or active, defence, were more likely to deter cyber incidents. This finding is linked to participants with a more appropriate and strong SA than participants who did not employ such methods. Such findings from the blue team capability condition experiments support the proposed research suggestion that use of offensive countermeasures in cyber defence is an effective strategy. Therefore, when SA is being aligned to doctrine then it enables cyber commanders to perform significantly better in tackling cyber attacks.

The effects of deception on participant SA, SA efficiency, SA efficacy, SA effectiveness, perception correctness, perception completeness, analysis capabilities, comprehension and confidence, the accuracy of captured information, timeliness of captured information, timeliness of awareness building, capability to act and respond and the capability to adapt to changes were also examined. It was evident that use of deception helped significantly to deter cyber incidents when participants appropriately utilised cyber deception capability conditions, compared with participants who did not. Thus, these findings help to also highlight the importance of cyber deception in cyber security and active defence. However, the results also indicate that deception capability should be used carefully and appropriately in order to maximise its advantages (stated above).

In conclusion, the results and findings confirm that active intelligence gathering using offensive hacking techniques enhance cyber situational awareness agility and quality in dealing with cyber incidents to a significant degree. In addition, it is clear that, when a winning attitude is adopted, participant situational awareness is statistically improved. Interestingly, participants with a military background managed to more effectively deter cyber incidents than those without one. In fact, situational awareness performance was better in participants with a military background: they became more agile in deterring cyber incidents (possibly due to their willingness to utilise both offensive methods and hacking skills). Finally, the results obtained from the blue team with offensive capabilities demonstrate that such a strategy is an important consideration with regards to producing an effective active defence strategy. A deception strategy in active cyber defence also appears to be a useful tool by which cyber commanders can defend their network. This method allows participants to buy extra time, enabling them to better understand cyber incidents, thus providing more control over the impact of these incidents. However, as previously stated, deception capability is a double-edged sword, and should be used carefully by cyber commanders.

CHAPTER 6: DISCUSSION AND CONCLUSION

6.0 OVERVIEW

The study has systematically explored the relevant and current literature and developments in the area of cyber SA. It has provided some insight by investigating the efficacy of the existing SA models and demonstrating their limitations in enhancing SA agility and quality. The topics covered also ranged from the legality and ethical considerations of Active SA up to the development of a technical test bed/environment.

In order to validate the proposed model and build this research theory, the study used Structure Equation Modelling (SEM), and this has afforded the research an opportunity to test whether active offensive intelligence gathering could enhance SA agility and quality when dealing with a cyber incident. The resulting SEM was then used to inform the development of the testing environment, where the proposed model would be tested in practice. In addition, the SEM result informed the development of a measurement instrument to measure SA performance objectively. After this, an independent sample T-test and ANOVA were used to test the effects of the following:

I. Active intelligence gathering and passive intelligence gathering conditions;
II. Influence of individual education (military and civilian background);
III. Utilisation of deception conditions; and
IV. Utilisation of blue team (control group) with offensive capabilities.

With all the above in mind, the research that effectively identified the current security needs of the cyber world and the shortcomings of the existing SA models and in turn allowed the study to introduce a new theory and theoretical framework that eventually shaped the new, Active SA Model.

The main outcome of this research is a novel and robust approach and theory for cyber SA where for the first time an active offensive intelligence activity is integrated into SA model which provides quality information that enhances the agility of awareness. So far all existing SA models discussed in literature were not doctrinally correct and passive in nature. This research developed the active SA model with an attitude to facilitate offensive intelligence gathering that aligns correctly with military doctrine. Also, the research provided a novel serious gaming environment as a robust testing environment that allowed this research to play a real cyber war in controlled environment without breaking the law. Finally, a novel SA assessment framework was developed to evaluate the efficiency, efficacy and effectiveness of cyber commanders' cyber SA which provided for the first time an objective means and method to quantify SA performance. This contribution provided a capability to determine where candidate's cyber training techniques may be improved. This chapter will discuss in detail contributions and outcomes of this research.

6.1 KEY FINDINGS:

Although there are many improvements and recommendations that this research has contributed, the key findings can be summarised as follows.

All current existence SA models are high-level models, are too general and are not doctrinally correct. They lack details about how SA should be performed, and consequently this research has helped advance the field of study by providing more real-life implementations and findings based on those models.

The research has also concluded that intelligence is a crucial factor in cyber SA, and its quality and timeliness do affect the performance of cyber SA. Active intelligence is a force multiplier that adds a new capability to the cyber commander. In turn this helps to achieve proper cyber SA through utilisation of offensive capabilities to influence the enemy and to be able to collect intelligence from within the enemy's domain.

This research has introduced active offensive intelligence gathering in an SA theory and model. This provides cyber commanders with additional intelligence from the enemy domain, rather than intelligence coming from local cyber security sensors. Therefore, the superior intelligence that comes from direct interaction with the enemy and intelligence from the enemy domain that relate to decision making helps decision makers to make the right decision and determine the right response to cyber incidents. Active SA, with its active offensive intelligence gathering, helps in enhancing cyber operations where commanders are always engaged in intelligence gathering. Being active in cyber space allows cyber commanders to collect information about potential targets and influence them before even they start attacking i.e. identifying the cyber threat early.

Deception is important for Active SA as it allows the defender to channel enemy attacks into a controlled environment where the defender can perform intelligence gathering and understand what the enemy is about to do. A deception service is considered a weapon, and can be used in Active SA to control the impact of cyber incidents and also to gather intelligence from an enemy, with the capacity to influence enemy decision-making and OODA loop. Therefore, training is crucial so defender utilise this method correctly.

Similarly, the use of a serious gaming environment is indeed a very useful tool for performing cyber SA, where it can be used to enhance people's capability through training. This environment allows users to reverse their decision and play real cyber-war games in a real controlled environment without breaching any laws. This research, with the use of a serious gaming environment, influences the current training techniques in practice. A serious gaming environment is a robust environment which can be used to enhance participants' performance in cyber security, and also can act as a platform for training and assessment.

As always, training is important for active cyber SA, and the military way of thinking is crucial to gain the advantage from this model and finally an Active SA model adds new capabilities to cyber commanders in which this method allows a defender to influence enemies and affect their decision making process and operate actively inside their OODA loop and out manoeuvre the enemy.

It is important to notice that, this thesis has highlighted the importance of offensive hacking and deception in enhancing cyber SA agility and quality. However, commanders should always remember that enemies could use deception and active offensive measures during cyber attacks. Therefore, they should always be prepared for similar incidents.

6.2 RESEARCH OBJECTIVES & ANALYSIS OUTCOMES

Objective 1: Determine and critically analyse the current SA models and identify the key dimensions and variables for Active cyber SA

Most recent studies on cyber SA have focused primarily on measuring the participants' cyber SA, without specifying how the cyber SA model components could be found (Stevens et al., 2013; Fink et al., 2013; Dutt et al., 2013). Although this is a useful field of study, there is great amount of perspective lost from not researching deeper the cyber SA model components themselves. In response, the current research has afforded the reader this view.

Another limitation of the extent research is data capture, in that most recent research has not specified the type of data to be gathered, but provided only a general outline of this critical process. With statistical analysis and conclusions being derived from data, this research has allocated more time to this critical process, with the objective of obtaining cleaner and more accurate results.

Lastly, and most critically, there is no research available that has discussed how the actual SA is performed, nor what the processes are for building cyber SA. One will also find that there is no model in the available literature that integrates, nor even includes, quality and agility aspects, which are critical elements that allow good cyber SA to be determined. In turn, available research is unable to describe how intelligence, quality and agility can be integrated into SA in order to produce superior and better SA.

Moreover, the main finding from the literature has been that all existing modules are high level and generalised models that do not focus on explaining how exactly SA can be performed or achieved in a practical, real life way. Also, existing modules were developed with the wrong attitude that were not doctrinally aligned which is not suitable for emerging cyber environment. This research has achieved the objective through critical examination of the current literature on non-cyber SA models (Endsley, 1995) and cyber related models (Tadda & JDL, 2008), concluding with a study into the Art of War. Computer forensic science was another critical part and, when combined with SA, it allowed the

research to develop a conceptual, hypothesised, active cyber SA model. The novel active SA theory was developed with due consideration given to aligning it with military doctrine and computer forensics capability so that a robust result in enhancing cyber SA agility and quality could be achieved.

Objective 2: Developing a theoretical framework for Active SA

To further assist in the development of the theoretical framework, a survey was conducted in which 271 cyber security experts participated, and then an exploratory factor analysis was conducted and structural equation applied to verify the Active SA model and it causal relations.

The purpose of this investigation was to determine whether active intelligence is more capable of providing enhanced security through enhanced active SA to cyber operators than passive intelligence. Active Intelligence (AI) as a construct can be defined as a package of both explicit and tacit knowledge (Nonaka, 1994; Nonaka & Nishiguchi, 2001) that directly affects SA quality and agility. On this point, the SEM for this study showed that AI activities significantly impacted on SA agility and quality, which in turn substantiates the claim that current and future cyber security measures should not omit adopting active defence techniques. By using SEM in order to validate this objective, the use of AI attests to the following statements:

I. It is crucial for the defender to interact with the enemy during a cyber incident in order to be able to identify the enemy's intention and motive;
II. It is crucial to obtain and exploit new knowledge during the cyber incident; and
III. When cyber commanders rely on intelligence coming from an enemy domain, rather than from local sensors alone, their SA is enhanced to a significant extent.

In respect to constructs such as Passive Intelligence (PI, which provides an enemy's IP address etc) and Intelligence Gathering (IG), the SEM showed that both are important to enhance overall SA agility and quality, as both are found to positively impact on SA and Active Intelligence (AI), since they provide the much-required direction to the AI for executing offensive attacks against enemy. It was also found that factors such as non-cyber intelligence and resource availability are no less crucial in enhancing SA agility and quality, as both are found to impact highly on PI, IG and AI. On this point, the study found that AI methods defined the principal capability at the core of the newly introduced SA model to deliver enhanced agility and quality in cyber SA.

Altogether, the SEM substantiated the basic premise of this study: that AI gathering activities significantly impact on SA agility and quality, and active defence techniques are indispensable for current future cyber security to enhance cyber defence against threats to CNI. This, however, also brings forth one important point, which is the need for enacting new laws and regulations at an international level to facilitate the gradual militarisation of cyberspace, which clearly is the order of the day, considering the high magnitude of hacking activities in term of cost and disruption.

The Role of Offensive Hacking in Enhancing Cyber SA Quality and Agility

Hacking, from the operator's end, requires applying more tactics and innovation, which in turn enhances the operator's agility in underpinning and exploiting the attacker's vulnerability. This leads to an incremental increase in the quality of cyber situational awareness (Endsley, 2000: 3). Perception, comprehension and projection are the three major drivers of situational awareness, which works at three levels. For example, perception of cues works as the initiator of required actions at the first level; comprehension of the situation helps the operator to effectively interpret the same at the second level; and this helps the operator to reach the projection level, i.e. to perform at the highest level of knowledge of cyber situation awareness. This shows that there is a complex degree of rigour involved in achieving and exploiting situation awareness, which in turn suggests that hacking helps to enhance the agility of the operators as hacking provides superior intelligence which assists in the prevention of cyber attacks.

One can arrive at the same conclusion from another perspective. Since the main task of the operators in protecting the network is to convert quality situation awareness into successful performance (Endsley, 2000), they must treat SA as a separate stage of functioning, because otherwise it becomes impossible to obtain quality SA, due to several intervening factors such as poor strategy selection, poor decision choices, technical constraints, inadequate training etc. In fact, the mutually supplementary roles of decision making and SA – decisions influenced by SA and SA influenced by decisions – strongly suggest that the entire process involves instant conversion of tacit knowledge into explicit knowledge (Nonaka, 1994; Nonaka & Nishiguchi, 2001), and the quality of SA projection is highly dependent on the operators' ability to effectively convert tacit knowledge into active knowledge within a split second. At this point, the significance of offensive intelligence gathering in achieving quality SA projection can be realised by considering the processes that act as the sources of both tacit and explicit knowledge by checking the enemy's attack process:

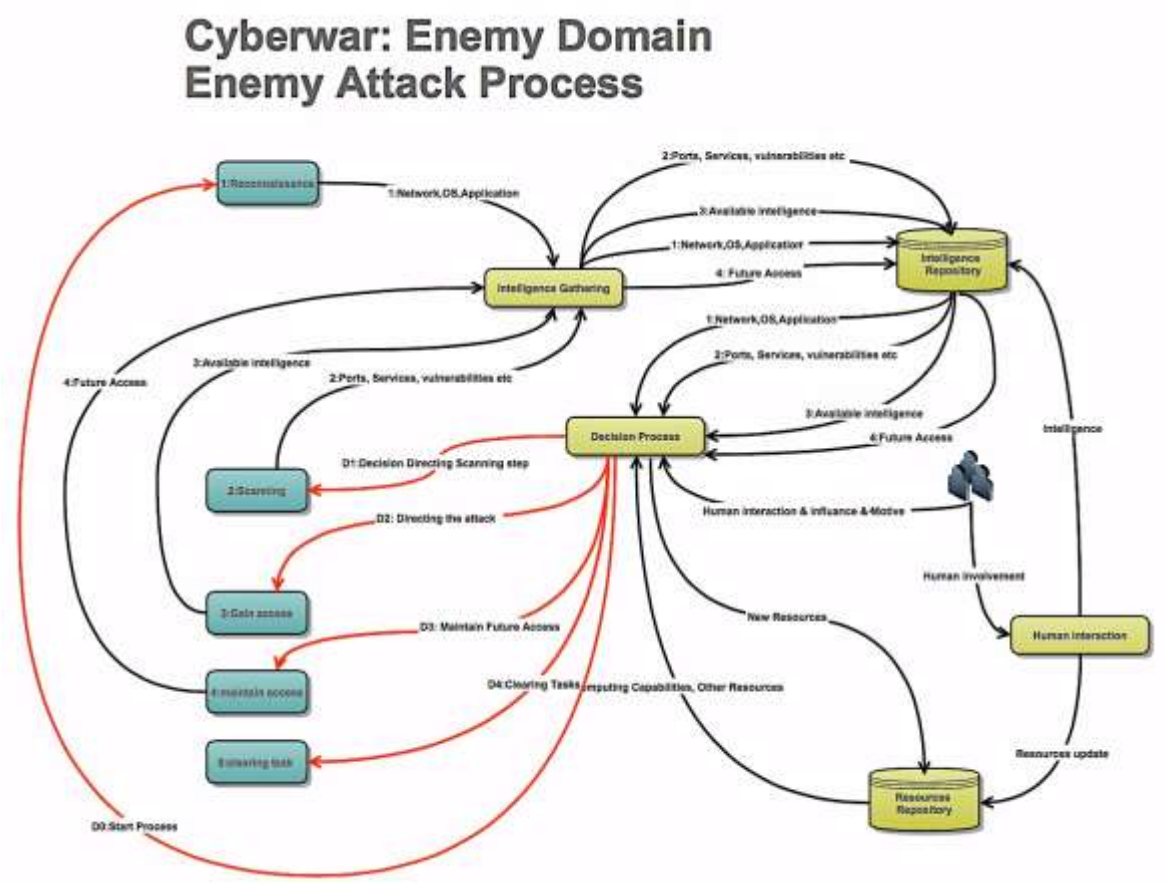


Figure 6.2: Enemy Attack Process (Source: Author)

The above diagram clearly highlights the fact that operators need to integrate the above processes with their own thought processes, as well as constantly synthesise them through the permutations and combinations of the various stages to obtain as many outcomes as possible. Therefore, it can said that ethical hacking acts as a much-required dynamic learning curve for the operators in order to keep them always alert, agile, fully aware of the latest trends of cyber attack and ready to deliver with innovative strategies. For this reason, Serious Gaming environment and active SA metrics should always be deployed to enhance cyber operator's capabilities through training.

At this point, it also becomes clear that operators require adequate training and other support, such as an appropriate infrastructure and a required amount of freedom, which will equip them to deal with all three levels of SA, i.e. perception, comprehension and projection, to the desired degree of intelligence and precision.

Objective 3: Evaluate Active SA deployment in a serious gaming environment

Following the findings of the literature review, which clearly posited the fact that active intelligence is an essential instrument for enhancing SA agility and quality, this study has introduced a new, enhanced situational awareness model that incorporates active offensive methods to extract active intelligence. This necessitated designing a new scale for SA; accordingly, new constructs have been added to the

model. Before, the SEM was used in the first stage to verify the theoretical model, the results of which were used in the second stage, to design:

1. Serious gaming environment;
2. SA behavioural anchor rating scheme; and
3. SA measurement and marking scheme based on ground truth.

In addition to the newly produced SA scale, the research needed an effective test bed. This came in the form of a "serious gaming environment", due to the fact that achieving SA requires the analyst to proceed through three stages: perception, comprehension and projection. The challenges of each of these stages are ingesting large volumes of data, sustaining real time response and presenting in a comprehensible format, respectively. Effective presentation of the current state allows the analyst to more rapidly identify anomalous behaviour and devise an appropriate response (Amico, 2005).

The rationale behind adopting serious gaming environment rests on the fact that traditional network SA tools such as Snort (www.snort.org), Nagios (www.nagios.org) or OpenNMS (www.opennms.org) eventually present volumes of logs and graphs of data in a variety of forms, such as streams of logs and scatter plots, bar charts, pie charts and graphs, which over time lose much of their meanings due to multiple dimensions emerging from information saturation.

On the other hand, a gaming environment provides a diverse suite of tools that enables the researcher to creatively depict asset behaviour, state and location. In addition, these tools enable the researcher to create a virtual world that accurately represents the real world, where accurate geo-location of assets helps the player to seamlessly identify the location of network assets that operate on the network. These facilitators eventually enable the player to perform actions to obtain pertinent information about the assets of interest, which in turn depict the accurate state of SA.

All the points above reinforce the importance of using a serious gaming environment, developed in this research using the Active SA model, as a crucial element to help test the research's main questions.

Lastly, it would be pertinent to mention at this point that, going by the available body of literature on SA, one finds that visualisation of SA has always been considered to be a prime precondition in measuring the state of SA. For example, Draper, Livnat & Riesenfeld (2008) recommend utilising visualisation techniques, after they identified its benefits through using their VisAlert intrusion detection technology, which enhanced their understanding of the state of SA among operators. Similarly, Glanfielf et al. (2009) used OverVlow to create FloVis, which is a visualisation tool for investigating network traffic. The framework of FloVis enables analysts to customise the entire analysis environment, which in turn allows them to better identify abnormal behaviour in the network under scrutiny. Altogether, the extant literature clearly identifies visualisation as the key to enhancing SA decision-making. Therefore, active SA theory inform the development of visualisation.

Objective 4: Develop a method framework for assessing cyber SA

In order to be able to assess theory in practice, the research developed assessment instruments that allow performance evaluation of Active SA theories in practice. The participants' SA performance was captured and evaluated with data gathered during the experiment. This allowed one to objectively mark the participants using a five-point Likert scale called SABARS, which was used for this research scenario and was subsequently validated during the pilot study by a group of cyber security experts.

This rating scale was developed by the researchers at the University of Queensland for measuring the SA performance of the members of the Air Services, Australia. SABARS enables expert observers to rate the SA performance of the operators at an individual level, with 28 behavioural checkpoints indexed to SA processes (Mathews et al., 2000). It uses a five-point Likert scale, where the performance on specified behaviours can be rated as either very poor, poor, borderline, good or very good. One view of the 28 framed SA behaviours suggests that it can also be generalised for other networks.

The rationale behind adopting SABARS rests on the fact that it encompasses almost all possible behaviours that can be associated with SA, and that it provides an easy way to identify the individual strength and weaknesses of the SA of each operator which in turn influence training technique and practice. Therefore, SABARS provides a solid basis for a behaviourally anchored rating (BARS) by assessing five broad areas of team-members' individual SA. At the same time, it also makes the job of the assessors much easier, as in this case the assessors only have to make five decisions about each operator to eventually capture the individual state of their SA (Campbell et al., 1973; Loughry, Ohland & Moore 2006). Altogether, SABARS offers several advantages, such as framing behavioural anchors within its rating scale, making the SA decision making processes easy and remaining unobtrusive, while helping assessors obtain a detailed measurement of all major individual SA behaviours of the operators. There are at least four other important points that go in favour of using SABARS, which enhance its reliability:

- One, it involves subject matter experts (SME) as assessors/observers to ensure the delivery of more reliable SA performance results of the operators;
- Two, it facilitates on-field SA assessments, where the observers have the scope to judge each participant within a real-life situation before rating their SA status; and
- Three, it is highly compatible with a C4i environment (Command, Control, Communication, Computers and Intelligence) (Salmon et al. 2006).
- Inform training techniques and practice.

In the case of this research, the result of the SABARS was then used to calculate participant SA performance, SA efficiency, SA efficacy and SA effectiveness using other metrics developed as a result of SEM and based on ground truth.

SA measurement and marking schemes based on ground truth: the rationale for using the marking scheme on ground truth is that it is virtually impossible to theoretically measure the intangible elements that build and activate SA, such as human "perception of the elements in the environment within a volume of space and time, the comprehension of their meaning, and the projection of their status in the near future" (Endsley, 2000: 3). Therefore, this research has novel contribution in being able to quantify SA performance.

Objective 5: Empirically assess the significance of effect and the implications of active defence in enhancing cyber SA agility and quality

As stated in chapter five, the main purpose of the experiment in this research study was to test the research hypothesis that active defence techniques are more capable of providing quality SA and ensuring greater degree of cyber security; this required examining the role of AI gathering by using offensive hacking techniques, and inferring from the outcomes of the tests whether active defence techniques are more capable of enhancing cyber situational awareness agility and quality in dealing with cyber incidents. Eventually, the finding was that participants' SA was significantly improved when a winning attitude (active offensive defence) introduced.

For example, the independent sample T-Test for active and passive conditions revealed that the active participants' total SA mean (M) improved by 32% (almost double) when they adopted a winning attitude, scoring higher than the passive control group. Similarly, Active participants' SA efficiency, efficacy and effectiveness were also increased by double when adopting a winning attitude. Moreover, the analysis reveals that SA perception, comprehension and SA projection were improved significantly in the case of the participants who belonged to the experiment group, which eventually enhanced each participant's agility and quality while dealing with cyber incidents. These findings, therefore, substantiate the fact that AI gathering using active offensive defence can enhance SA agility and quality. Active SA model provides greater capability in providing quality cyber security.

The outcome of the T-test showed that active defence techniques enhanced the overall SA performance of the participants by 32%, and that the participants who operated with a winning attitude scored a higher SA. This therefore implies that constant patrolling in cyberspace to detect, deny, pursue and destroy the attackers' ploys have made the participants totally engaged in cyber operations, and such engagement has developed their ability to constantly gather tacit knowledge and convert the same into explicit knowledge in less time, which, in other words, can be described as an intrinsic process of developing SA agility and quality. The above view accords with the observation of Varon (2002) that the best defence is a strong offense, since in this case the operators are engaged in the constant lookout for any malicious activities in cyberspace. Altogether, the findings of the T-test clearly substantiate the fact that active defence techniques should be an integral part of any cyber security initiative, much in the mould of the old adage that prevention is better than cure.

The second finding from the T-test, i.e. participants' SA efficiency, efficacy and effectiveness were enhanced 2 times better when adopting a winning attitude, clearly substantiates the fact that a military doctrine highly complements active defence techniques which advocate an active defence posture. A winning attitude can be defined as a proactive approach, which is an essential element of any military strategy and which perfectly suits the context of this study, since cyber attacks virtually resemble the real-life attacks intended to capture or dominate the opponent's space and to rule over the defeated network. A winning attitude in this case follows a cycle of activities that goes through two stages:

Constantly applying prior knowledge along with new knowledge
Constantly engaging the attacker in deciphering this new knowledge

Therefore, the efficacy of a winning attitude recorded in the T-test not only clearly endorses the above strategy as best practice in any cyber security initiative, but also endorses the theoretical framework of the active defence technique that has been applied in active SA theory:

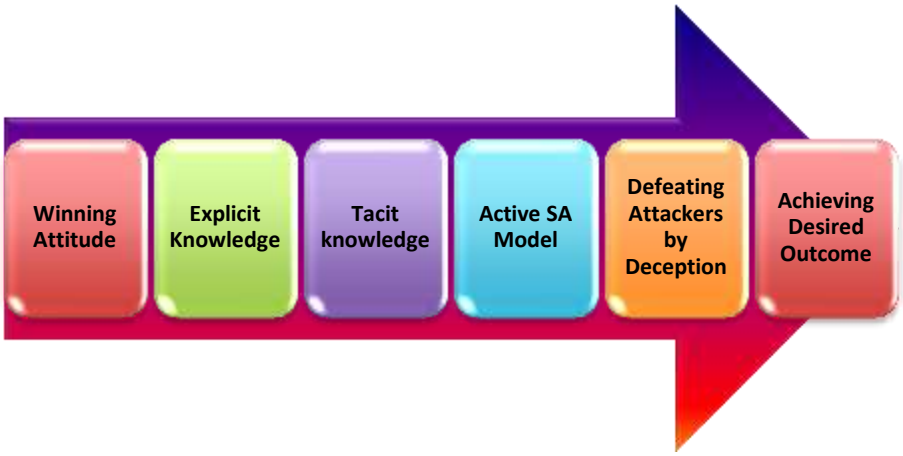


Figure 6.1: Active SA in Context (Source: Author)

The above diagram shows that an active defence technique is guided by three drivers – a winning attitude (Active offensive defence posture), explicit knowledge and tacit knowledge – which together create a force that is superior to the attacker, and eventually that force is projected through an Active SA Model to defeat the attacker and achieve the desired outcome, i.e. keeping the network fully free from any attack. It is here that the various roles of the Active SA theory also come to the fore, since in the absence of those roles the participants could not have increased their SA efficiency, efficacy and effectiveness by 35%. Its roles thus can be framed in the following manner:

I. The new active SA model facilitates interaction with the adversaries;
II. It gets activated once an attack gets redirected;
III. It uses deception (new knowledge for the attacker) through redirecting the attacker to deception server;
IV. It controls the adversaries and enters into their domain through all possible means;
V. It captures the attackers within a deception loop and keeps them fully busy there (i.e. busy in deciphering the constant barrage of new knowledge).

The above roles performed in Active SA Model can be distributed among the four categories of military strategy as suggested by Sun Tzu: Initiation, Direction, Action and Exploitation. Equally, it becomes clear from the above state of affairs that new knowledge, being the prime instrument of military strategy, acts here as the force multiplier within the newly introduced active SA model, where intelligence generated from new knowledge plays a big role in creating and applying the new knowledge.

The proven efficacy of the Active SA Model also serves as a pointer to its indispensability in securing important networks, especially when one learns that any cyber security initiative from a military/strategic point of view needs to address at least eight interrelated variables, which are political, military, economic, social, information, infrastructure, physical environment and time (TRADOC, 2010), and to address the following eight issues to build its safety framework:

I. Identity (at least cyber identity) of the attacker
II. Motive of the attacker
III. Location of the attacker
IV. Goal of the attacker
V. Weakness of the attacker
VI. Possible impact of attack on the operator's domain
VII. Ways to defuse the attack before its occurrence

Thus, it has been determined through survey and experimentation that the success of the new Active SA Model has been demonstrated in practice because of the fact that it has successfully integrated the military philosophy of Sun Tzu in its structure and mechanisms, as well as successfully addressed the above variables recommended by the US Army in its cyberspace security plans for 2016-2018 (TRADOC, 2010). In fact, a 35% increase in SA efficiency, efficacy and effectiveness among the participants demonstrates a high increase in SA agility and quality, since SA efficiency, efficacy and effectiveness eventually culminate in improved SA agility and quality. Since no cyber security initiative can do without SA agility and quality, the proven ability of Active SA Model thus easily makes its mark by enhancing the SA performance of the participant operators who have adopted a winning attitude and correctly used deception techniques. Even a brief discussion on the role of agility and quality obviates why the new Active SA Model should be considered indispensable for its ability to enhance SA agility and quality for delivering superior active SA in contemporary active defence environments.

The second independent sample T-test, assessing participants' background (military and non-military), was conducted to explore the impact of a military way of thinking on using active defence techniques and dealing with cyber incidents. The results of this test showed that those who have a military way of thinking are better equipped to deter cyber incidents than their counterparts. Here, the mean in participants' total SA difference stood at 24%, i.e. the performance of the participants with a military

way of thinking was found to be 24% better than those who came from a non-military background. In addition, the participants with a military background were found to be more agile in deterring cyber incidents, which strongly suggests that their willingness to adopt a winning attitude and to exploit the offensive methods act as the main drivers in enhancing their SA skills.

Another test was conducted in this study – a one-way ANOVA – to examine the impact of utilisation of the blue team with offensive capabilities and the utilisation of deception. The findings from this test showed that utilisation of offensive capabilities improved participants' overall SA to a significant extent, which clearly suggests that participants' SA performance was highly impacted by the active defence technique, as well as validating offensive capability as the major driver of SA performance. In regard to deception, the outcome of the analysis showed that participants who utilised deception service correctly were able to perform much better than those who did not. The findings also revealed the following points:

- The deception service enabled the participants to gain extra time to thoroughly scrutinise and comprehend the cyber incidents;
- As a consequence, the participants successfully utilising the deception service were able to control the cyber incidental impact easily and in less time; and
- Incorrect utilisation of deception leads to failure in controlling cyber incidents and ends up with poor SA performance.

The above points clearly articulate two facts: one, a deception technique is an essential tool that operators can use to remain one up against the cyber attackers; two, failure to utilise a deception technique can be fatal for the security system, and therefore operators should possess appropriate knowledge and training to successfully utilise the same. While the second point involves factors of human error, which can be resolved with the help of knowledge and training, the first point clearly shows that deception techniques are an integral part of the overall active defence technique.

The study has shown that correct utilisation of deception with a winning attitude has considerably enhanced the SA of operators and cyber commanders alike. This finding corroborates the findings of the experts, who explain the correlation between enhanced SA performance and deception by suggesting that deception enables the operator to buy more time in many ways, which the operators can exploit in order to learn about the attacker in detail. For example, an operator might adopt techniques such as hiding information about a network's topology, its vulnerabilities and its assets from a hacker's reconnaissance by intercepting connections to unused network addresses or by impersonating computers, where its ruses (tricks designed to deceive) would make it difficult for the attackers to identify the real computers and/or scan the network without avoiding detection. This shows that deception can be used both by hiding and showing techniques, where in the first case deception conceals or obscures certain elements of the network, and in the second case it shows something that does not exist (Bell & Whaley, 1992; Yull, Denning & Feer, 2006). In addition, an extremely

important point emerges from the seminal work of Yull et al. (2006), which is that the central tenet of the deception technique is to defeat the attacker, who is considered to be a discovery agent, and whose failure to discover the hidden thing should be attributed to the superior knowledge and skills of the operator. This statement perfectly suits the finding of this study, i.e. that the operator should possess a winning attitude (will to defeat), and should opt for offensive methods/techniques to protect the network.

Participant Feedback Result Discussion

In order to be certain about participants' evaluation and feedback regarding the new model and its security features, this research asked participants several questions about the Active SA model, deception, the serious gaming environment and offensive capabilities. The results of this observation were positive, as participants considered the introduced model as a blueprint for future cyber SA security that would shape the structure of future cyber security technologies and platforms. Further to this, participants found that the Active model and its variables were very simple and easy to understand, and that this could be a very useful guidance for cyber security personnel in dealing with cyber attacks due to the fact that this model's variables tell what data are to be collected, where to find them and how to extract them. Some of participants, in fact, believed that this model could allow the organisation to assess its security team and help in drawing up the right training program to enhance the cyber security capability.

The serious gaming environment in the experiment showed a very resourceful tool to achieve the enhancement through assessment of an organisation's security and the application of a real experiment to assess people and their capabilities in dealing with cyber incidents so that proper training can be provided, which they believed it is essential for the Active SA model so the organisation can get the full advantages out of Active SA system. The cyber deception service in the serious gaming environment, which is basically a clone of real resources, grabbed the participants' attention, who found it to be a very useful and resourceful tool, especially when compared with the current honeypot technologies. Their cumulative comments about this service were positive, and they found that this cloned service provides cyber security personnel with more time and greater capability to understand enemy intentions while controlling the magnitude of the cyber attack. When asked if they found this feature useful going forwards, they believed it was indeed a very promising technique, as it is very difficult to detect compared with low-level interaction currently used in honeypots, which can be detected by the enemy. A point they wished to note, however, was that although the deception as a cloned service provides real interaction with the system, the enemy they were interacting with was ultimately controlled by a cyber security team.

In general, participants indicated that cyber deception can be implemented at a national level to ensure the security of the nation's critical assets. Finally, participants believed that interaction with the enemy during a cyber incident is crucial for Active SA, as such interactions would provide the defender with superior intelligence to defeat enemy courses action. The offensive capabilities could be utilised in

future to protect national assets and defeat the enemy during a cyber war, but this depends on the maturity of the law and the situation where counter attacks and cyber self defence are covered.

6.3 THEORETICAL AND METHODOLOGICAL CONTRIBUTION

This research study contributes a novel theory and framework to the cyber situational awareness literature that enhances cyber SA in cyber security, and identifies the variables that explain this cyber active SA model. Also, this research adds for the first time the notion of active intelligence and quality and agility to the cyber SA model, and a valid scale to measure it. Albert (2006) argues that better SA should rely on good intelligence, and this shows how important active intelligence is in enhancing cyber SA. This is due to the fact that active intelligence gathers more information about adversaries in order to make intelligence more complete for the defender.

The main contributions of this research are:

I. A theory for active cyber SA and its implementation in practice.
II. An objective assessment framework and approaches to evaluate the operator's performance of cyber SA
III. An active defence process that explain how to apply active SA theory into practice.

This research has contributed into the body of knowledge by providing a detailed framework that explains how enhanced cyber SA in cyber security could be achieved assessed and how it could be enhanced. All previous models discussed previously are too general and lack detail about how cyber SA can be achieved. Information about what data cyber commanders should find are not covered; there are only general ideas about how to monitor network assets, which makes current methods passive and inadequate for dealing with cyber attacks. The passive approach adopted currently is not adequate for cyber security, because defenders simply wait for cyber incidents and then react. Such an approach provides only one side of intelligence: one that is simply controlled by adversaries. Active intelligence using an offensive approach has been introduced in this research to enhance cyber SA by providing additional intelligence from the enemy's domain through active interaction with the enemy's attack. This approach shows significant enhancement in cyber SA and cyber security.

The active cyber SA theory in this research includes active intelligence, quality and agility as the main components of SA, as this research believes that no cyber SA can be achieved without having reliable sources of intelligence to build agile and quality SA. In addition, this research study makes a significant contribution to the cyber SA literature by introducing new and valid constructs, namely active intelligence, quality and agility. This study is the first that has integrated and used these constructs in a new theory for cyber SA that truly enhances cyber SA and cyber defence capabilities in deterring cyber incidents and in turn provides the mean to objectively measure the performance of SA through quality and agility construct variables. Another major contribution made is to the cyber SA and cyber defence literature by providing a rich explanation of how active offensive capabilities provide advantages into cyber defence operations in practice by enhancing cyber SA while dealing with cyber incidents.

Previously, cyber SA and SA in general were measured either in subjective or less objective ways to assess people's SA when dealing with an event. However, current metrics were designed for a non-cyber domain, and so do not necessary explain how SA can be achieved. This research adopted non-intrusive techniques to collect information on expert involvement in cyber incidents, which are then used to assess participant SA using a behavioural anchor rating scale based on the ground truth already identified in the experiment scenario. The results of both previous instruments were then fused into cyber SA assessment framework employing the metrics developed based on a SEM to measure participants' cyber SA performance. Therefore, this research added novelty in the area of assessing cyber SA where the introduced metric and method used in this research allowed for the first time to quantify cyber SA performance. Given that Cyberspace, as one of the global commons(air, maritime, space, land, cyber) (MNE7, 2013), underpins and is critical to the functioning of the other global commons used in the defence of critical national infrastructure then active SA theory and application has a critical role to play in enhancing SA for many stakeholders.

In addition, this research provided another novel methodological contribution shaped in a serious gaming environment designed for the purpose of assessing cyber SA. The main advantage of this environment is that it allows us to mimic a real-life cyber network and cyber attack scenarios in a controlled network environment without breaking laws. This environment is simply a cloned network asset built in to a virtualised environment that allows the research to play a cyber attack game with a group of experts to assess their SA performance in dealing with cyber incidents in real life. Moreover, the impact of this novelty has an important effect in training techniques and practice as this environment allows organisation to assess their personnel and determine where a candidate's cyber training, techniques and practice may be improved.

Finally, this research has verified and validated the active SA theory through utilising the power of structural equation modelling and then has been validated through an intensive lab experiment as discussed using cyber security experts whom they provided accreditation to this research contribution. The developed and demonstrated active SA theory and practice has shown significant in cyber SA performance dramatically in term of efficiency, efficacy and effectiveness which cannot be ignored.

6.4 RESEARCH LIMITATIONS

The following section discusses the main limitations of this research study. First, due to limited resources in the area of cyber SA and Active defence the research tries to apply different techniques, such as military and forensic science, in order to develop the theoretical Active cyber SA defence framework. Also, cyber SA models in the literature are too general to show how these models should be performed. There is no clear discussion on how different SA components interrelate, and not enough information on the data gathering process.

Second, the measurement of cyber SA in the literature is mainly focused in measuring SA itself, and ignores the measurement of the quality of each process and agility in acquiring it.

Thirdly, it is interesting to note that human error has been found to be one of the most significant sources of susceptibility in any secure information system. This research is about developing a cyber situational awareness through exploiting network and system data to determine the existence of cyber attacks. Therefore, human error as discussed above is out of this research scope.

Active offensive Cyber SA is required for future cyber security and cyber defence. However, in order to achieve the desire protection, defenders are required to have enough knowledge about the enemies. This can be achieved by continues patrolling in cyberspace to identify the potential attackers. Also, having distributed sensors and predication tools are important so deception and offensive measures can be deployed against detected incidents. Training is required as active SA personnel should have enough knowledge in the area of hacking and defence in order to perform correctly. Finally, Active SA is a great deal but it is useful to protect a national infrastructure due to fact, offensive measures and action should be granted and supported by law so cyber commanders won't be prosecuted for their actions.

This research adopted five Likert scale in both stage one survey and stage two lab experiment SA BARS due to the fact that the Likert Scale is a well known method for survey collection and is also easy to understand. However, respondents to such scale may interpret it differently from one another which could cause problems in the result. Another problem found when using Likert scale is that the space between each choice cannot be identified so that space is ignored. Therefore, this research considered the above discussed points as a limitation in this research.

Finally, it would be useful to have a greater range of scenarios to test out the active SA theory and practice more extensively as well as addressing how active SA theory can address contemporary and emerging cyber threats. This will be addressed in future research where CNI such as telecom will be considered to test the active SA theory and practice.

6.5 FUTURE WORK

Quantum computing is the next era of computing, first theorised by Argonne National Laboratory. Paul Benioff created the first quantum computer theory in 1981, which is basically based on the power of atoms and molecules to perform processing tasks and memory. Quantum computing is a promising area, where the speed of processing will significantly increase much faster than current silicon based computers.

With this in mind, it is envisioned that future research will focus on studying the impacts of quantum computing on the Active SA model and how this technology can be exploited to enhance the model's capabilities and performance. Quantum computing will add new capabilities to cyber security. The speed of processing data will enhance the speed of detection, speed of capturing data and speed of processing large amounts of data, and finally will enhance the prediction. However, the question is:

how could this affect the intelligence gathering process in the Active SA model, and how agile is Active SA in deterring cyber incidents?

Quantum computing has the potential to allow future research to design a robust and agile data gathering machine that spreads into different sources to gather intelligence, which then can be fused into a neural-like network to process the data quickly and efficiently, so that quality predictions and decisions can be made. These assumptions will require more research, so the aim of any future work will focus on studying the possibility of exploiting quantum computing to enhance the cyber security SA and maybe come to an idea about setting up a quantum cyber security SA platform.

This study confirms the importance of Active SA model in enhancing cyber agility and quality to enhance cyber security. However, this study didn't cover the cost of such adoption comparing with the benefit so as future work, the cost effective of Active SA model will be conducted.

In the near future it would also be beneficial to develop a live system that can be used against real hackers/enemies in a parallel live environment. The idea would be that such an implementation would help improve the system and related models over time, to be able to bootstrap a system or theoretical implementation with an established knowledge database. This would allow future implementations to start with a concrete and up to date knowledge base, as opposed to learning the new techniques from scratch with each system iteration and/or deployment.

6.6 Concluding Remarks

Whilst it might be generally agreed that Active SA has its merits, it is still important to note that the respective legislation needs to sanction its greater use. It is hoped that this study affords interested parties a greater look into the practical applications of using Active SA in the cyber arena. Whilst respecting the necessity for literature and theoretical modelling, this research bridges a capabilities gap between the theoretical and practical usages of active SA and delivers a superior active SA prototype for active cyber defence.

REFERENCES:

Achinstein, P. (1968). *Concepts of science: A philosophical analysis*. Johns Hopkins Press Baltimore.

Adams, M. (1990). Hacker's Heaven. *Science News*, *138*(21), 323. doi:10.2307/3974809

Adams, M. J., Tenney, Y. J., & Pew, R. W. (1995). Situation awareness and the cognitive management of complex systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 85–104.

Addinall, R. (2012). Information in Warfare from Sun Tzu to the "War on Terror,." In *Security and Defence: National and International Issues, 7th Annual Graduate Student Symposium* (pp. 457–477).

Aitoro, J. R. (2009, October 2). Terrorists nearing ability to launch big cyberattacks against U.S. Retrieved November 29, 2013, from http://www.nextgov.com/technology-news/2009/10/terrorists-nearing-ability-to-launch-big-cyberattacks-against-us/44951/

Alavi, M., & Carlson, P. (1992). A review of MIS research and disciplinary development. *Journal of Management Information Systems*, *8*(4), 45–62.

Albanesius, C. (2012). Military and Government Access to Your Data? House Clashes over CISPA. *Law and Legislation, Vol. 6(2)*: 1-4.

Albanesius, C. (2012b). Facebook Defends CISPA, Denies Plans to Share User Data. *Journal of Contemporary Technology, Vol. 3(5)*: 1-5.

Alberts, D.S., Garstka, J.J.and Stein, F.P. (2002) *Network-Centric Warfare: Developing and Leveraging Information Superiority (2nd ed. Vol. 2):* CCRP Publication series

Alberts, C., Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2004). *Defining incident management processes for csirts: A work in progress*. DTIC Document.

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). Introduction to the OCTAVE Approach. *Pittsburgh, PA, Carnegie Mellon University*.

Alberts, D. S., Garstka, J. J., & Stein, F. P. (2000). *Network Centric Warfare: Developing and Leveraging Information Superiority.* DTIC Document.

Alberts, D. S., & Hayes, R. E. (2006). *Understanding Command and Control*.

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers & Security*, *26*(4), 276–289.

Alcorn, W., Frichot, C., & Orru, M. (2014). *The Browser Hacker's Handbook*. John Wiley & Sons.

Amin, S., Schwartz, G. A., & Hussain, A. (2013). In quest of benchmarking security risks to cyber-physical systems. *IEEE Network*, *27*(1), 19–24. doi:10.1109/MNET.2013.6423187

Andersen, N. B. (1985). Conference review: IS Research–A Doubtful Science. *Research Methods in Information Systems, Elsevier Science, Amsterdam*.

Arnould, E. J. (1998). Daring consumer-oriented ethnography. *Representing Consumers: Voices, Views and Visions*, 85–126.

Arsene, L. (2009, September 19). U.S. to Apply Self-Defense Rule if Cyber Attacks Turn Hostile. *HOTforSecurity*. Retrieved December 3, 2013, from http://www.hotforsecurity.com/blog/u-s-to-apply-self-defense-rule-if-cyber-attacks-turn-hostile-3550.html

Artefact Group. (2012). Artefact- Technology Product Design and Development for the 21st Century. *Artefact*. Retrieved December 4, 2013, from http://www.artefactgroup.com/

Baratz, A., & GMT, 2:00am. (2004, November 12). Malware: what it is and how to prevent it. *Ars Technica*. Retrieved November 29, 2013, from http://arstechnica.com/security/2004/11/malware/

Barber, R. (2001). Hackers profiled—who are they and what are their motivations? *Computer Fraud & Security*, *2001*(2), 14–17.

Bartusik, K., & Cabala, P. (1997). Metoda scenariuszy w planowaniu strategicznym. *Przegl\kad Organizacji*, (2), 20–25.

Bass, T. (2000). Cyberspace situational awareness demands mimic traditional command requirements. *SIGNAL-FALLS CHURCH VIRGINIA THEN FAIRFAX–*, *54*(6), 83–84.

Baxter, G. D., & Bass, E. J. (1998). Human error revisited: Some lessons for situation awareness. In *Human Interaction with Complex Systems, 1998. Proceedings., Fourth Annual Symposium on* (pp. 81–87).

Bayuk, J. L. (2011). Systems security engineering. *Security & Privacy, IEEE*, *9*(2), 72–74.

Beaver, J. M., Steed, C. A., Patton, R. M., Cui, X., & Schultz, M. (2011). Visualization techniques for computer network defense (Vol. 8019, pp. 801906–801906–9). doi:10.1117/12.883487

Beaver, K. (2007). *Hacking for dummies*. John Wiley & Sons.

Bedny, G., & Meister, D. (1999). Theory of activity and situation awareness. *International Journal of Cognitive Ergonomics*, *3*(1), 63–72.

Bellacqua, J. A., & Hartnett, D. M. (2013). *Article by LTG Qi Jianguo on International Security Affairs*. CENTER FOR NAVAL ANALYSES ALEXANDRIA VA.

Bentler, P. M., & Chou, C.-P. (1987). Practical issues in structural modeling. *Sociological Methods & Research*, *16*(1), 78–117.

Bhaskar, R. (2006). State and local law enforcement is not ready for a cyber katrina. *Communications of the ACM*, *49*(2), 81–83.

Bickel, P., & Doksum, K. (1977). Mathematical Statistics Holden-Day. *Inc., SF*.

Biros, D. P., & Eppich, T. (2001). THEME: SECURITY-Human Element Key to Intrusion Detection. *Signal-Fairfax*, *55*(12), 31–34.

Bitdefender Labs. (2012). FLAME – The Story of Leaked Data Carried by Human Vector. *Bitdefender Labs*. Retrieved November 29, 2013, from http://labs.bitdefender.com/2012/06/flame-the-story-of-leaked-data-carried-by-human-vector/

Bollen, K. A. (1989). *Structural equations with latent variables*. New York: Wiley.

Börjeson, L., Höjer, M., Dreborg, K.-H., Ekvall, T., & Finnveden, G. (2006). Scenario types and techniques: towards a user's guide. *Futures*, *38*(7), 723–739.

Boyd, J. R. (1987a). *A discourse of winning and losing*.

Boyd, J. R. (1987b). Organic design for command and control. *A Discourse on Winning and Losing*.

Boyer, W., & McQueen, M. (2008). Ideal Based Cyber Security Technical Metrics for Control Systems. In J. Lopez & B. M. Hämmerli (Eds.), *Critical Information Infrastructures Security* (pp. 246–260). Springer Berlin Heidelberg. Retrieved from http://link.springer.com/chapter/10.1007/978-3-540-89173-4_21

Bradley, T. (2006). *Essential Computer Security: Everyone's Guide to Email, Internet, and Wireless Security: Everyone's Guide to Email, Internet, and Wireless Security*. Syngress.

Brenner, S. W. (2010). *Cybercrime criminal threats from cyberspace*. Santa Barbara, CA: Praeger.

Breton, R., & Rousseau, R. (2003, February 5). Situation Awareness: A Review of the Concept and its Measurement. Defence R&D Canada - Valcartier. Retrieved from http://pubs.rddc-drdc.gc.ca/BASIS/pcandid/www/engpub/DDW?W%3DAUTHOR+%3D+%27Breton%2C+R.%27%26M%3D8%26K%3D518754%26U%3D1

Browne, M. W., & Cudek, R. (1993). *Alternative Ways of Assessing Model Fit in Bollen, KA, and Long, JS Testing Structural Equation Models*. Newbury Park, CA, Sage.

Bryman, A. (1988). *Quantity and quality in social research*. London; Boston: Unwin Hyman.

Bryman, A., & Bell, E. (2007). *Business research methods*. Oxford university press.

Burgoon, J. K., & Buller, D. B. (1994). Interpersonal deception: III. Effects of deceit on perceived communication and nonverbal behavior dynamics. *Journal of Nonverbal Behavior*, *18*(2), 155–184.

Byrne, B. (2010). Structural Equation Modelling Using AMOS. *Basic Concepts, Applications, and Programming*.

Byrne, B. M. (2001). Structural equation modeling with AMOS, EQS, and LISREL: Comparative approaches to testing for the factorial validity of a measuring instrument. *International Journal of Testing*, *1*(1), 55–86.

Cahanin, S. E. (2011). *Principles of War for Cyberspace*. DTIC Document.

Campbell, J. P., Dunnette, M. D., Arvey, R. D., & Hellervik, L. V. (1973). The development and evaluation of behaviorally based rating scales. *Journal of Applied Psychology*, *57*(1), 15.

Cardinal, C. N. (2000). *Delivering joint information superiority*. DTIC Document.

Carr, J. (2011). *Inside cyber warfare: Mapping the cyber underworld*. O'Reilly.

CBS. (2009). "60 Minutes"--Cyberwar: Sabotaging the system. *CNET*. Retrieved November 29, 2013, from http://news.cnet.com/8301-1009_3-10393170-83.html

Chen, C. C., Medlin, B. D., & Shaw, R. (2008). A cross-cultural investigation of situational information security awareness programs. *Information Management & Computer Security*, *16*(4), 360–376.

Chen, J., Tan, R., Xing, G., Wang, X., & Fu, X. (2012). Fidelity-Aware Utilization Control for Cyber-Physical Surveillance Systems. *IEEE Transactions on Parallel and Distributed Systems*, *23*(9), 1739–1751. doi:10.1109/TPDS.2012.74

Chen, T. M. (2010). In cyber space, big brothers are watching you [Editor's Note]. *Network, IEEE*, *24*(1), 2–3.

Chen, T. M., & Robert, J. (2004). The Evolution of Viruses and Worms. *STATISTICAL METHODS IN COMPUTER*. Retrieved from http://citeseer.uark.edu:8380/citeseerx/viewdoc/summary?doi=10.1.1.115.639

Cherryholmes, C. H. (1992). Notes on pragmatism and scientific realism. *Educational Researcher*, *21*(6), 13–17.

Chik, W. B., & Bartholomew, W. (2007). Challenges to Criminal Law Making in the New Global Information Society: A Critical Comparative Study of the Adequacies of Computer-Related Criminal Legislation in the United States, the United Kingdom and Singapore. *Cybercrime and the Law (Icfai Law Books)*.

Chin, W. W. (1998). The partial least squares approach for structural equation modeling.

Chow, S.-C., Wang, H., & Shao, J. (2003). *Sample Size Calculations in Clinical Research*. CRC Press.

Churchill Jr, G. A. (1979). A paradigm for developing better measures of marketing constructs. *Journal of Marketing Research*, 64–73.

CISCO. (2012). What Is the Difference: Viruses, Worms, Trojans, and Bots? *Cisco*. Retrieved November 29, 2013, from http://www.cisco.com/web/about/security/intelligence/virus-worm-diffs.html

Clausewitz, C. von. (1976). *On War, ed. and trans. M. Howard and P. Paret*. Princeton, NJ: Princeton University Press.

Clarke, R. (2009). Categories of malware in support of malware policy analysis. *Canberra: Xamax Consultancy*. Retrieved from http://www.rogerclarke.com/II/MalCat-0909.html [accessed 8 August 2012].

Cody, E. (2007, September 13). Chinese Official Accuses Nations of Hacking. *Washington Post*. US. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2007/09/12/AR2007091200791.html

Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences (2nd Edition). Hillsdale, NJ: Lawrence Earlbaum Associates.

Committee on Deterring Cyber attacks. (2010). *Proceedings of a workshop on deterring cyberattacks: informing strategies and developing options for U.S. policy*. Washington, D.C: National Academies Press.

Coolican, H. (2004). *Research methods and statistics in psychology* (4th ed.). London: Hodder & Stoughton.

Coram, R. (2002). *Boyd: The fighter pilot who changed the art of war*. Hachette Digital, Inc.

Cox, E.P. (1986). The optimal number of response alternatives for a scale: A review. *Journal of Marketing Research', 17(4) pp. 407-422*

Crotty, M. (1998). *The foundations of social research: Meaning and perspective in the research process*. Sage.

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 49, pp. 229–233).

Da-Yu, K., & Shiuh-Jeng, W. (2009). The IP address and time in cyber-crime investigation. *Policing: An International Journal of Police Strategies & Management*, *32*(2), 194–208. doi:10.1108/13639510910958136

Davison, R. (1998). An action research perspective of group support systems: how to improve meetings in Hong Kong. *Unpublished PhD Dissertation, City University of Hong Kong*.

Dawes, J., & others. (2002). Five point vs. eleven point scales: does it make a difference to data characteristics. *Australasian Journal of Market Research*, *10*(1).

DeLooze, L. L. (2008). Counter hack: Creating a context for a cyber forensics course. In *Frontiers in Education Conference, 2008. FIE 2008. 38th Annual* (p. T2H–1).

Denning, D. E. (1987). An intrusion-detection model. *Software Engineering, IEEE Transactions on*, (2), 222–232.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy. *Networks and Netwars: The Future of Terror, Crime, and Militancy*, 239–288.

Devault, G. (2012). Choosing Between Qualitative and Quantitative Methods. Retrieved January 16, 2014, from http://marketresearch.about.com/od/market.research.techniques/a/Choosing-Between-Qualitative-And-Quantitative-Methods.htm

Devine, S. (2010). Stuxnet may be the work of state-backed hackers. *Network Security*, *2010*(9), 1–2. doi:10.1016/S1353-4858(10)70111-2

DHS. (2010). U.S. Army Cyberspace Operations Concept Capability Plan 2016-2028 | Public Intelligence. Retrieved from http://publicintelligence.net/u-s-army-cyberspace-operations-concept-capability-plan-2016-2028/

Dominguez, C., Vidulich, M., Vogel, E., & McMillan, G. (1994). *Situation awareness: Papers and annotated bibliography. Armstrong Laboratory, Human System Center, ref*. AL/CF-TR-1994-0085.

download. (n.d.). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.63.1478&rep=rep1&type=pdf

Draper, G., Livnat, Y., & Riesenfeld, R. (2008). A visual query language for correlation discovery and management. In *Proc. Second Ann. Visual and Iconic Language Conf.(VaIL'08)* (pp. 14–23). Citeseer.

Durso, F. T., Hackworth, C. A., Truitt, T. R., Crutchfield, J., & Nikolic, D. (1999). *Situation Awareness As a Predictor of Performance in En Route Air Traffic Controllers.*

Dutt, V., Ahn, Y.-S., & Gonzalez, C. (2013). Cyber Situation Awareness Modeling Detection of Cyber Attacks With Instance-Based Learning Theory. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *55*(3), 605–618.

Dwyer, D. (2009). Chinese cyber-attack tools continue to evolve. *Network Security*, *2009*(4), 9–11.

Easterby-Smith, M., Thorpe, R., Jackson, P., & Lowe, A. (2008). *Management research*. Sage.

Eichin, M. W., & Rochlis, J. A. (1989). With microscope and tweezers: An analysis of the internet virus of november 1988. In *Security and Privacy, 1989. Proceedings., 1989 IEEE Symposium on* (pp. 326–343).

Eisenhardt, K. M. (1989). Building theories from case study research. *Academy of Management Review*, *14*(4), 532–550.

Elden, M., & Chisholm, R. F. (1993). Emerging varieties of action research: Introduction to the special issue. *Human Relations*, *46*(2), 121–142.

Ellen, O. (2012). Cyber Security without Cyber War. *Journal of Conflict and Security Law*, *17*(2), 187–209. doi:10.1093/jcsl/krs017

Emm, D. (2012). Cybercrime and the law: a review of UK computer crime legislation. *securelist.com*. Retrieved January 15, 2014, from http://www.securelist.com/en/analysis/204792064/Cybercrime_and_the_law_a_review_of_UK_computer_crime_legislation

Endsley, M. (1989a). Final report: Situation awareness in an advanced strategic mission (NOR DOC 89-32). *Hawthorne, CA: Northrop Corporation*.

Endsley, M. (1989b). Tactical simulation 3 test report: Addendum 1 situation awareness evaluations (81203033R). *Hawthorne, CA: Northrop Corporation*.

Endsley, M. (1990a). A methodology for the objective measurement of pilot situation awareness. *AGARD, Situational Awareness in Aerospace Operations 9 p(SEE N 90-28972 23-53)*.

Endsley, M.R. (1993). Situation awareness in dynamic human decision making: *Theory and measurement. Los Angeles, CA: University of Southern California.*

Endsley, M. R. (1995b). A taxonomy of situation awareness errors. *Human Factors in Aviation Operations*, 287–292.

Endsley, M. R. (1995a). Measurement of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 65–84.

Endsley, M. R. (1995c). Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 32–64.

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 32, pp. 97–101).

Endsley, M. R. (1990). Predictive utility of an objective measure of situation awareness. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 34, pp. 41–45).

Endsley, M. R. (2000). Theoretical underpinnings of situation awareness: A critical review. *Situation Awareness Analysis and Measurement*, 3–32.

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

Endsley, M. R., & Kiris, E. O. (1995). The Out-of-the-Loop Performance Problem and Level of Control in Automation. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(2), 381–394. doi:10.1518/001872095779064555

Endsley, M. R., & Robertson, M. M. (1996). Team situation awareness in aviation maintenance. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 40, pp. 1077–1081).

Endsley, M. R., & Rodgers, M. D. (1994). Situation awareness information requirements analysis for en route air traffic control. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 38, pp. 71–75).

Endsley, M. R., Selcon, S. J., Hardiman, T. D., & Croft, D. G. (1998). A comparative analysis of SAGAT and SART for evaluations of situation awareness. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 42, pp. 82–86).

Endsley, M., Sollenberger, R., & Stein, E. (1999). The Use of Predictive Displays for Aiding Controller Situation Awareness. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *43*(1), 51–55. doi:10.1177/154193129904300111

Entin, E. E., Hiniker, P., Grier, R., Jefferson, T., Vecchio, G., & Harkins, J. (2006). Enhancing Situational Awareness and Team Performance Using Network Centric Technologies. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 50, pp. 482–486).

Erbetta, J. (2003). *Attrition in network centric warfare*. DTIC Document.

Erickson, J. (2008). *Hacking: The art of exploitation*. No Starch Press.

Eun, Y.-S., & Abmann, J. S. (2014). Cyberwar: Taking Stock of Security and Warfare in the Digital Age. *International Studies Perspectives*.

Fabrigar, L. R., Wegener, D. T., MacCallum, R. C., & Strahan, E. J. (1999). Evaluating the use of exploratory factor analysis in psychological research. *Psychological Methods*, *4*(3), 272.

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1), 23–40.

Feakin, T. (2013). Enter the Cyber Dragon: understanding Chinese intelligence agencies' cyber capabilities.

Field, A. P. (2005). *Discovering statistics using SPSS: (and sex, drugs and rock "n" roll)* (2nd ed.). London ; Thousand Oaks, Calif: Sage Publications.

Fink, G., Best, D., Manz, D., Popovsky, V., & Endicott-Popovsky, B. (2013). Gamification for Measuring Cyber Security Situational Awareness. In *Foundations of Augmented Cognition* (pp. 656–665). Springer.

Flach, J. M. (1995). Situation awareness: Proceed with caution. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 149–157.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 39–50.

Fracker, M. L. (1991). *Measures of situation awareness: Review and future directions*. DTIC Document.

Fulghum, D. A. (2006). Redefining victory. *Aviation Week and Space Technology*, *165*(10), 58–58.

Fulghum, D. A., Wall, R., & Butler, A. (2007). Cyber-Combat's First Shot. *Aviation Week & Space Technology*, *167*(21), 28–31.

Futures Group (1994). Statistical modelling - From time series to simulation. *United Nations University, Washington D.C., USA*

GAO Reports. (2000). Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000: *T-AIMD-00-229. GAO Reports, 22nd Feb. 2000; 14.*

Galliers, R. (1992). *Information systems research: issues, methods, and practical guidelines*. Oxford; Boston: Blackwell Scientific Publications.

Geers, K. (2007). Greetz from Room 101 (pp. 1–24). Presented at the DEF CON, Black Hat.

Geers, K. (2011). *Strategic Cyber Security*. ccdcoe Press. Retrieved from http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF

Gefen, D., Straub, D. W., & Boudreau, M.-C. (2000). Structural equation modeling and regression: Guidelines for research practice. In *Communications of the Association for Information Systems*.

George, J. F., Easton, G. K., Nunamaker, J., & Northcraft, G. B. (1990). A study of collaborative group work with and without computer-based support. *Information Systems Research*, *1*(4), 394–415.

Georgala, K., Kosmopoulos, A., & Paliouras, G. (2014). Spam Filtering: an Active Learning Approach using Incremental Clustering. In *Proceedings of the 4th International Conference on Web Intelligence, Mining and Semantics (WIMS14)* (p. 23). ACM.

Geweke, J. F., & Singleton, K. J. (1980). Interpreting the likelihood ratio statistic in factor models when sample size is small. *Journal of the American Statistical Association*, *75*(369), 133–137.

GILES, M. L. (n.d.). *SUN TZU ON THE ART OF WAR, THE OLDEST MILITARY TREATISE IN THE WORLD. Trans-lated from the Chinese with Introduction and Critical Notes by LIONEL GILES, MA, Assistant in the Department of Oriental Printed Books and MSS. in the British Museum, First Published in 1910. 1910*.

Ginovsky, J. (2012, June 1). Cyber attacks are soaring. How to thwart them - ABA Banking Journal. Retrieved January 15, 2014, from http://www.ababj.com/component/k2/item/3779-cyber-attacks-are-soaring-how-to-thwart-them

Glaser, B. G. (1998). *Doing grounded theory: Issues and discussions* (Vol. 254). Sociology Press Mill Valley, CA.

GLASER, B., & STRAUSS, A. (1967). *The Discovery of Grounded Theory: strategies for qualitative research (Chicago, IL, AVC)*. Chicago.

GMA. (2012, June 2). New "Flame" spyware could be next super cyberweapon –Kaspersky, ITU. *GMA News Online*. Retrieved December 2, 2013, from http://www.gmanetwork.com/news/story/260375/scitech/technology/new-flame-spyware-could-be-next-super-cyberweapon-kaspersky-itu

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). *2005 CSI/FBI computer crime and security survey*. Computer Security Institute.

Gordon, S. (2005). Geographic flexibility will boost prospects. *Computer Weekly*, 54–54.

Gorman, S. (2013, July 22). Annual U.S. Cybercrime Costs Estimated at $100 Billion. *Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10001424127887324328904578621880966242990

Gorman, S. (2009, May 7). FAA's Air-Traffic Networks Breached by Hackers. Retrieved December 2, 2013, from http://online.wsj.com/news/articles/SB124165272826193727

Goulding, C. (2005). Grounded theory, ethnography and phenomenology: A comparative analysis of three qualitative strategies for marketing research. *European Journal of Marketing*, *39*(3/4), 294–308.

Grazioli, S., & Jarvenpaa, S. L. (2003). Deceived: under target online. *Communications of the ACM*, *46*(12), 196–205.

Greenwald, C. (2012, September 19). Various matters: cyberwar, last gasps, and hate speech. *the Guardian*. Retrieved December 3, 2013, from http://www.theguardian.com/commentisfree/2012/sep/19/cyberwar-last-gasps-hate-speech

Greenwald, G., & MacAskill, E. (2013). Obama orders US to draw up overseas target list for cyber-attacks. *The Guardian*.

Greetz from Room 101 - dc-15-geers-WP.pdf. (n.d.). Retrieved from http://www.defcon.org/images/defcon-15/dc15-presentations/Geers/Whitepaper/dc-15-geers-WP.pdf

Grimaila, M. R., & Fortson, L. W. (2007). Towards an information asset-based defensive cyber damage assessment process. In *Computational Intelligence in Security and Defense Applications, 2007. CISDA 2007. IEEE Symposium on* (pp. 206–212).

Grow, B., Elgin, B., & Herbst, M. (2006). Click Fraud: The dark side of online advertising. *BusinessWeek Online*, *10*(02).

GuideStar Communication. (2003). Overview of Qualitative and Quantitative Research in Measuring Organizational Communications - Article by GuideStar Communications. Retrieved January 16, 2014, from http://www.guidestarco.com/Qualitative-and-Quantitative-Survey-Research.HTM

Hair, J. F. (2006). *Multivariate data analysis* (6th ed.). Upper Saddle River, N.J: Pearson Prentice Hall.

Hair, J. F., Tatham, R., & Black, W. (1998). *Multivariate data analysis*. Upper Saddle River, N.J: Prentice Hall.

Hair, J., Black, B., Babin, B., & Anderson, R. (2010). Multivariate Data Analysis 7th Pearson Prentice Hall. *Upper Saddle River, NJ*.

Hall, D. L., & Llinas, J. (1997). An introduction to multisensor data fusion. *Proceedings of the IEEE*, *85*(1), 6–23.

Hansman, S., & Hunt, R. (2005). A taxonomy of network and computer attacks. *Computers & Security*, *24*(1), 31–43.

Hariri, S., Qu, G., Dharmagadda, T., Ramkishore, M., & Raghavendra, C. S. (2003). Impact analysis of faults and attacks in large-scale networks. *Security & Privacy, IEEE*, *1*(5), 49–54.

Harrald, J., & Jefferson, T. (2007). Shared situational awareness in emergency management mitigation and response. In *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on* (pp. 23–23).

Hartley, S. L., & MacLean, W. (2006). A review of the reliability and validity of Likert-type scales for people with intellectual disability. *Journal of Intellectual Disability Research*, *50*(11), 813–827.

HBGary. (2013). Active Defense. *HBGary*. Retrieved December 2, 2013, from http://hbgary.com/products/active_defense

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105.

Himma, K. E., & Tavani, H. T. (2008). *The handbook of information and computer ethics*. Wiley. com.

Hirschheim, R. (1985). Information systems epistemology: An historical perspective. *Research Methods in Information Systems*, 13–35.

Hoaglin, D. C., & Iglewicz, B. (1987). Fine-tuning some resistant rules for outlier labeling. *Journal of the American Statistical Association*, *82*(400), 1147–1149.

Hoaglin, D. C., Iglewicz, B., & Tukey, J. W. (1986). Performance of some resistant rules for outlier labeling. *Journal of the American Statistical Association*, *81*(396), 991–999.

Hollinger, R., (1998). Computer hackers follow a Guttmann-like progression. *Sociology and Social Research 72:199-200.*

Holdaway, E. J. (2001). *Active Computer Network Defense: An Assessment*. DTIC Document.

Holden, M. T., & Lynch, P. (2004). Choosing the appropriate methodology: understanding research philosophy. *The Marketing Review*, *4*(4), 397–409.

House of Commons Defense Committee. (2013). Defense and Cyber-Security: Government Response to the Committee's Sixth Report of Session 2012-13. *Sixth Special Report of Session 2012-13.*

Hu, J., & Jiang, F. (2012). Preface of the "Workshop on computational intelligence and cyber security." *AIP Conference Proceedings*, *1479*, 1492–1493. doi:10.1063/1.4756447

Huerta, L. A., d' Entremont, C., & González, M.-F. (2006). Cyber charter schools: Can accountability keep pace with innovation? *Phi Delta Kappan*, *88*(1), 23–30.

Huey, L., & Rosenberg, R. S. (2004). Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention. *Canadian Journal of Criminology and Criminal Justice*, *46*(5), 597.

Husserl, E. (1965). Phenomenology and the crisis of philosophy: Philosophy as a rigorous science, and philosophy and the crisis of European man.

Information Warfare Monitor. (2009). Tracking GhostNet: Investigating a Cyber Espionage Network (Vol. JR02–2009 Tracking GhostNet). Ottawa Canada: Ghostnet. Retrieved from http://www.nartv.org/mirror/ghostnet.pdf

Jajodia, S., Noel, S., Kalapa, P., Albanese, M., & Williams, J. (2011). Cauldron mission-centric cyber situational awareness with defense in depth. In *MILITARY COMMUNICATIONS CONFERENCE, 2011-MILCOM 2011* (pp. 1339–1344).

Jaquith, A. (2007). *Security metrics: replacing fear, uncertainty, and doubt*. Addison-Wesley Upper Saddle River.

Järvinen, P. (2007). Action research is similar to design science. *Quality & Quantity*, *41*(1), 37–54.

Jasper, S. (2012). *Conflict and cooperation in the global commons: a comprehensive approach for international security*. Washington, DC: Georgetown University Press.

Johnson, C. W. (2013). Anti-social networking: crowdsourcing and the cyber defence of national critical infrastructures. *Ergonomics*, (ahead-of-print), 1–15.

Jones, D. G., & Endsley, M. R. (1996). Sources of situation awareness errors in aviation. *Aviation, Space, and Environmental Medicine*.

Jones, K. J., Bejtlich, R., & Rose, C. W. (2006). *Real digital forensics: computer security and incident response*. Upper Saddle River, NJ: Addison-Wesley.

JW, C. (2003). *Research design: Qualitative, quantitative, and mixed method approaches*. Sage Publications.

Kates Jr, D. B. (1992). Second Amendment and the Ideology of Self-Protection, The. *Const. Comment.*, *9*, 87.

Kaplan, B., & Maxwell, J. (1994). Evaluating health care information systems: Methods and applications. *Qualitative Research Methods for Evaluating Computer Information Systems. JG Anderson, CE Ayden and SJ Jay. Thousand Oaks, Sage*.

Kaplan, J. A. (2012, May 29). Powerful "Flame" cyberweapon torching Mideast computers. *FoxNews.com*. Text.Article. Retrieved December 2, 2013, from http://www.foxnews.com/tech/2012/05/29/world-most-sophisticated-cyber-weapon-burns-computers-in-middle-east/

Kaser, D. (2012). Where Privacy Meets Security. *Information Today*, *29*(8), 3–3.

Kaspersky Lab. (2012). Kaspersky Lab and ITU Research Reveals New Advanced Cyber Threat. Retrieved January 15, 2014, from http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Research_Reveals_New_Advanced_Cyber_Threat

Kelliher, F. (2005). INTERPRETIVISM AND THE PURSUIT OF RESEARCH LEGITIMISATION: AN INTEGRATED APPROACH TO SINGLE CASE DESIGN. *The Electronic Journal of Business Research Methodology*, *3*(2), 123–132.

Kent, K., Mell, P., & Nusbaum, J. (2005). *Guide to malware incident prevention and handling: Recommendations of the National Institute of Standards and Technology*. US Department of Commerce, National Institute of Standards and Technology.

Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). *State of the practice of computer security incident response teams (CSIRTs)*. DTIC Document.

Kjaerland, M. (2005). A classification of computer security incidents based on reported attack data. *Journal of Investigative Psychology and Offender Profiling*, *2*(2), 105–120.

Klein, G. (2000). Cognitive task analysis of teams. *Cognitive Task Analysis*, 417–429.

Krathwohl, D. R. (1997). *Methods of educational & social science research: an integrated approach* (2nd ed.). New York: Longman.

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educ Psychol Meas*.

Kuhn, T. S. (1970). The structure of scientific revolutions. *Chicago/London*.

Lachow, I. (2013). *Active Cyber Defense: A Framework for Policymakers*. US: Center for a New American Security. Retrieved from http://www.cnas.org/publications/policy-briefs/active-cyber-defense-a-framework-for-policymakers

Lee, D. (2014, March 5). Cyber "stand-off" in Ukraine crisis. *BBC*. Retrieved from http://www.bbc.co.uk/news/technology-26447200

Lehr, W. H., & Pupillo, L. M. (2009). *Internet Policy and Economics: Challenges and Perspectives*. Springer.

Lewis, R., Louvieris, P., Abbott, P., Clewley, N., & Jones, K. (2014). CYBERSECURITY INFORMATION SHARING: A FRAMEWORK FOR SUSTAINABLE INFORMATION SECURITY MANAGEMENT IN UK SME SUPPLY CHAINS.

Lewis, J. A. (2002). *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Center for Strategic & International Studies.

Li, J., Ou, X., & Rajagopalan, R. (2010). Uncertainty and risk management in cyber situational awareness. In *Cyber Situational Awareness* (pp. 51–68). Springer.

Limpanitgul, T., Robson, M., & Soreze, F. (2009). *Methodological considerations in a quantitative study examining the relationship between job attitudes and citizenship behaviors*. 18th EDAMBA Summer Academy, Soreze, France.

Lincoln, Y. S., & Guba, E. G. (2000). y EG Guba 2000."Paradigmatic Controversies, Contradictions, and Emerging Confluences,." *NK Denzin E Yvonna S., Lincoln (eds.), Handbook of Qualitative Research. London: Sage*.

Loader, B. D., & Thomas, D. (2013). *Cybercrime: Security and surveillance in the information age*. Routledge.

Lobel, H. (2012). Cyber War Inc.: The Law of War Implications of the Private Sector's Role in Cyber Conflict. *Tex. Int'l LJ*, *47*, 617–617.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to information systems: today's reality, yesterday's understanding. *MIS Quarterly*, 173–186.

Loughry, M. L., Ohland, M. W., & Moore, D. D. (2007). Development of a theory-based assessment of team member effectiveness. *Educational and Psychological Measurement*, *67*(3), 505–524.

Lugosky, J., & Dove, R. (2011). Identifying Agile Security Patterns in Adversarial Stigmergic Systems. In *Twenty-First Annual International Symposium of INCOSE, Denver, CO (US), June* (pp. 20–22).

Luzwick, P. (2000). Situational Awareness and OODA Loops: Coherent Knowledge-based Operations Applied: Last in a series of 4 articles. *Computer Fraud & Security*, *2000*(4), 15–17. doi:10.1016/S1361-3723(00)04017-3

MacCallum, R. C., Browne, M. W., & Sugawara, H. M. (1996). Power analysis and determination of sample size for covariance structure modeling. *Psychological Methods*, *1*(2), 130.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*, *15*(4), 251–266.

Masip, J., Garrido, E., & Herrero, C. (2004). Defining deception.

Matthews, M. D., Pleban, R. J., Endsley, M. R., & Strater, L. D. (2000). Measures of infantry situation awareness for a virtual MOUT environment. In *Proceedings of the 1st Human Performance, Situation Awareness and Automation Conference*.

Maykut, P., & Morehouse, R. (2002). *Beginning qualitative research: A philosophical and practical guide*. Routledge.

Maykut, P. S. (1994). *Beginning qualitative research: a philosophic and practical guide*. London ; Washington, D.C: Falmer Press.

McCarty, B. (2003). The honeynet arms race. *Security & Privacy, IEEE*, *1*(6), 79–82.

McClure, S., Scambray, J., Kurtz, G., & Kurtz. (2005). *Hacking exposed: network security secrets and solutions*. McGraw-Hill/Osborne New York.

McDaniel, C. D., & Gates, R. H. (2013). *Marketing research essentials*. Hoboken, N.J.; Chichester: Wiley ; John Wiley [distributor].

McGraw, G. (2013). Cyber War is Inevitable (Unless We Build Security In). *Journal of Strategic Studies*, *36*(1), 109–119. doi:10.1080/01402390.2012.742013

McGuinness, B., & Foy, L. (2000). A subjective measure of SA: the Crew Awareness Rating Scale (CARS). In *Proceedings of the first human performance, situation awareness, and automation conference, Savannah, Georgia*.

McKinnon, D. P. (2008). *Introduction to statistical mediation analysis*. New York: Taylor and Francis Group.

McLuhan, M. (1994). *Understanding media: The extensions of man*. MIT press.

Meilinger, P. S. (1995). *10 Propositions Regarding Air Power*. DTIC Document.

Meserve, J. (2007). Sources: Staged cyber attack reveals vulnerability in power grid. *CNN. Com*, *26*.

Milhorn, H. T. (2007). *Cybercrime: How to avoid becoming a victim*. Universal-Publishers. com.

Mishra, P., & Eich, M. H. (1992). Join processing in relational databases. *ACM Computing Surveys (CSUR)*, *24*(1), 63–113.

Mishra, S. (2003). Network centric warfare in the context of "operation Iraqi freedom." *Strategic Analysis*, *27*(4), 546–562.

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human element of security*. Wiley. com.

MNE7. (2013, February 25). Concept of Employment for Cyber Situational Awareness Within the Global Commons. Version 1.0. MNE7. Retrieved from http://mne.oslo.mil.no:8080/Multinatio/MNE7produk/35CyberCon/file/3.5%20Concept%20of%20Employment.pdf

Molander, R. C., Riddile, A., Wilson, P. A., & Williamson, S. (1998). *Strategic information warfare: A new face of war*. Rand Corporation.

Moore, T., Friedman, A., & Procaccia, A. D. (2010). Would a'cyber warrior'protect us: exploring trade-offs between attack and defense of information systems. In *Proceedings of the 2010 workshop on New security paradigms* (pp. 85–94).

Morgan, D. L. (1998). Practical strategies for combining qualitative and quantitative methods: Applications to health research. *Qualitative Health Research*, *8*(3), 362–376.

Muller, H. S. (2008). What is Spam? Spam Abuse.net. Retrieved from http://spam.abuse.net/overview/whatisspam.shtml (Accessed on 19/05/2013)

Muniz, E., Stout, R., Bowers, C., & Salas, E. (1998). A methodology for measuring team situational awareness: situational awareness linked indicators adapted to novel tasks (SALIENT). *NATO Human Factors and Medicine Panel on Collaborative Crew Performance in Complex Systems, Edinburgh, North Atlantic Treaties Organisation, Neuilly-Sur-Seine*, 20–24.

Myers, M. D. (1997). Qualitative research in information systems. *Management Information Systems Quarterly*, *21*, 241–242.

Nakashima, E. (2010). Defense official discloses cyberattack. *Washington Post*, *24*.

NASA: Human-Centered Systems Lab (2006). NASA Ames Research Center, CA retrieved from: http://human-factors.arc.nasa.gov/ihi/hcsl/sadisplays.html.

Neuman, L., & others. (2000). Social research methods: qualitative and quantitative approaches. *Allyn &Bacon*.

Neumann, L. (1983). Effects of scale length on means and correlation coefficients. *Quality & Quantity*, *17*(5), 405–408.

Noman, H. (2011). The emergence of open and organized pro-government cyber attacks in the Middle East: The case of the Syrian Electronic Army. *Information Warfare Monitor*.

NOMIKOS, J. M. (2005). A European Union Intelligence Service for Confronting Terrorism. *International Journal of Intelligence and CounterIntelligence*, *18*(2), 191–203. doi:10.1080/08850600590911936

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science*, *5*(1), 14–37.

Nonaka, I., & Nishiguchi, T. (2001). Social, Technical and Evolutionary Dimensions of Knowledge Creation". *Knowledge Emergence: Social, Technical, and Evolutionary Dimensions of Knowledge Creation*, 286.

Norman, H. (2011). 'The Emergence of Open and Organized Pro-Government Cyber Attacks in the Middle East: The Case of the Syrian Electronic Army.' *OpenNet Initiative Bulletin [online] available from https://opennet.net/emergence-open-and-organized-pro-government-cyber-attacks-middle-east-case-syrian-electronic-army* [accessed 12 November 2013].

Nye Jr, J. S. (2011). *Nuclear lessons for cyber security*. DTIC Document.

O'Connell, M. E. (2012). Cyber Security without Cyber War. *Journal of Conflict and Security Law*, *17*(2), 187–209.

O'Reilly, T. (2005). *What is web 2.0, design patterns and business models for the next generation of software. Retrieved December 1, 2008*.

Odell, J. (1998). QUALITATIVE RESEARCH DESIGN. Retrieved January 16, 2014, from http://www3.uakron.edu/arm/resources/general_social_science/SYLLABUS%20QUALITATIVE%20RESEARCH%20DESIGN,%20University%20of%20Southern%20California%20IH2.pdf

Onwubiko, C. (2009). Functional requirements of situational awareness in computer network security. In *Intelligence and Security Informatics, 2009. ISI'09. IEEE International Conference on* (pp. 209–213).

Opala, O. J., & Rahman, S. S. M. (2013). CORPORATE ROLE IN PROTECTING CONSUMERS FROM THE RISK OF IDENTITY THEFT. *International Journal of Computer Networks & Communications*, *5*(5).

Orr, R. (2007) 'Computer voting machines on trial.' Knight Rider Tribune Business News 2 August.

Palermo, G. B., & Kocsis, R. N. (2005). *Offender Profiling: An Introduction to the Sociopsychological Analysis of Violent Crime*. Charles C Thomas Publisher.

Park, R. C., & Duggan, D. P. (2001). Principles of Cyber-warfare. IEEE.

Parish, S., & Goostree, P. (2013). *System and method for tracking computer viruses*. Google Patents.

Patrick Howell O'Neill. (2013, November 2). How the first botnet changed the Internet forever. *The Daily Dot*. Retrieved November 29, 2013, from http://www.dailydot.com/crime/robert-morris-botnet-virus-changed-internet/

Patton, M. Q. (1990). *Qualitative evaluation and research methods* . SAGE Publications, inc.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77.

Perry, C. (1998). A structured approach for presenting theses. *Australasian Marketing Journal (AMJ)*, *6*(1), 63–85.

Pesonen, H.-L., Ekvall, T., Fleischer, G., Huppes, G., Jahn, C., Klos, Z. S., … others. (2000). Framework for scenario development in LCA. *The International Journal of Life Cycle Assessment*, *5*(1), 21–30.

Peterson, D. (2013). Offensive Cyber Weapons: Construction, Development, and Employment. *Journal of Strategic Studies*, *36*(1), 120–124.

Peters, M., & Robinson, V. (1984). The origins and status of action research. *The Journal of Applied Behavioral Science*, *20*(2), 113–124.

Phillips, D., & Burbules, N. C. (2000). *Postpositivism and educational research*. Rowman & Littlefield Publishers.

Preimesberger, C. (2006). PLUGGING HOLES-Worried about security breaches in your IT infrastructure? So are the Red Teams at Sandia National Laboratories. It's their responsibility to protect the US IT infrastructure and thwart cyberterrorists. *PC Week*, *3*, 18.

Preston, C. C., & Colman, A. M. (2000). Optimal number of response categories in rating scales: reliability, validity, discriminating power, and respondent preferences. *Acta Psychologica*, *104*(1), 1–15.

Poursaberi, A., Yanushkevich, S., Gavrilova, M. L., Shmerko, V. P., & Wang, P. S. (2013). Situational awareness through biometrics. *Computer*, *46*(5), 0102–104.

Prouty, L. F. (2011). *The secret team: the CIA and its allies in control of the United States and the world*. Skyhorse Publishing Inc.

Ransome, J., & Misra, A. (2013). *Core Software Security: Security at the Source*. CRC Press.

Remenyi, D., & Williams, B. (1996). The nature of research: qualitative or quantitative, narrative or paradigmatic? *Information Systems Journal*, *6*(2), 131–146.

Robillard, N. (2004) Diffusing a logic bomb. Seattle: SANS Institute

Rona, T. P. (1976). Weapon systems and information war. *Boeing Aerospace Co., Seattle, WA*.

Rosce, J. T. (1975). Fundamental research Statistics for the behavioural Sciences. *New York*.

Ross, M. E., Narayanan, N. H., Hendrix, T. D., & Myneni, L. S. (2011). The Pragmatist in Context of a National Science Foundation Supported Grant Program Evaluation: Guidelines and Paradigms. *Journal of MultiDisciplinary Evaluation*, *7*(16), 111–130.

Rowe, N. C. (2004). A model of deception during cyber-attacks on information systems. In *Multi-Agent Security and Survivability, 2004 IEEE First Symposium on* (pp. 21–30).

Rowe, N. C., & Rothstein, H. S. (2004). Two taxonomies of deception for attacks on information systems.

Rubin, H. J. (1995). *Qualitative interviewing: the art of hearing data*. Thousand Oaks: Sage Publications.

Rudner, M. (2013). Cyber-Threats to Critical National Infrastructure: An Intelligence Challenge. *International Journal of Intelligence and CounterIntelligence*, *26*(3), 453–481.

Russel, K. (2004, January 19). QuickStudy: Phishing. *Computerworld*. Retrieved December 2, 2013, from http://www.computerworld.com/s/article/89096/Phishing

Salerno, J. J., Blasch, E. P., Hinman, M., & Boulware, D. M. (2005). Evaluating algorithmic techniques in supporting situation awareness. In *Defense and Security* (pp. 96–104).

Salerno, J. J., Tadda, G., Boulware, D., Hinman, M., & Gorton, S. (2005). Achieving situation awareness in a cyber environment. In *Proc of the Situation Management Workshop of MILCOM*.

Salerno, J. J., & Tadda, G. P. (2009). *Ranking Activities Based on Their Impact and Threat*. DTIC Document.

Salmon, P. M., Stanton, N. A., Walker, G. H., Jenkins, D., Ladva, D., Rafferty, L., & Young, M. (2009). Measuring Situation Awareness in complex systems: Comparison of measures study. *International Journal of Industrial Ergonomics*, *39*(3), 490–500. doi:10.1016/j.ergon.2008.10.010

Salmon, P., Stanton, N., Walker, G., & Green, D. (2006). Situation awareness measurement: A review of applicability for C4i environments. *Applied Ergonomics*, *37*(2), 225–238.

Samaha, J. (2005). *Criminal Justice With Infotrac*. CengageBrain. com.

Sanford, N. (1970). Whatever happened to action research? *Journal of Social Issues*, *26*(4), 3–23.

Saraswat, L., Yadav, P. S., & Rani, R. (2010). Adaptability of IEEE 802.15. 4 (Zigbee) Protocol for Wireless Sensor network. *IJCSE) International Journal on Computer Science and Engineering*, *2*(03), 554–559.

Sarter, N. B., & Woods, D. D. (1995). How in the World Did We Ever Get into That Mode? Mode Error and Awareness in Supervisory Control. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 5–19. doi:10.1518/001872095779049516

Saunders, M., Lewis, P., & Thornhill, A. (2007). Research Methods for Business Students (4: e uppl.) Harlow: Pearson Education.

Sawyer, R. D. (1994). *Sun-tzu: The art of war*. Basic Books.

Scheb, J. M. (2012). *Criminal law* (6th ed.). Belmont, CA: Wadsworth.

Schechtman, G. M. (1996). *Manipulating the OODA Loop: The Overlooked Role of Information Resource Management in Information Warfare.* DTIC Document.

Schell, B. H., & Martin, C. (2004). *Cybercrime: a reference handbook*. ABC-CLIO.

Schermelleh-Engel, K., & Werner, C. (2009). Introduction to Structural Equation Modeling with LISREL: Advantages, Challenges, and Problems. *Goethe University, Frankfurt (1-4)*.

Schiffman, L., & Kanuk, L. (1997). Consumer Behaviour (pp. 558-583). *Prentice-Hall, Englewood Cliffs, NJ*.

Schiller, J. (2010). *Cyber Attacks and Protection: Civilization Depends on Internet and Email*. CreateSpace.

Schmoldt, A., Benthe, H. F., & Haberland, G. (1975). Digitoxin metabolism by rat liver microsomes. *Biochemical Pharmacology*, *24*(17), 1639–1641.

Schütz, A. (1967). *The phenomenology of the social world*. Northwestern Univ Press.

Schwandt, T. A. (1994). Constructivist, interpretivist approaches to human inquiry.

Sekaran, U., & Bougie, R. (2000). *Research methods for business: A skill-building approach. NYC: John Willey Sons*. Inc.

Shah, R., & Goldstein, S. M. (2006). Use of structural equation modeling in operations management research: Looking back and forward. *Journal of Operations Management*, *24*(2), 148–169.

Shimeall, T., Williams, P., & Dunlevy, C. (2001). Countering cyber war. *NATO Review*, *49*(4), 16–28.

Sinha, K., Kemerlis, V., Pappas, V., Sethumadhavan, S., & Keromytis, A. D. (2014). Enhancing Security by Diversifying Instruction Sets.

Silverman, D. (2000). *Doing qualitative research: a practical handbook Sage Publications*. London.

Simon, H. A. (1981). *The sciences of the artificial, 1981*. MIT Press.

Skoudis, E., & Liston, T. (2005). *Counter hack: a step-by-step guide to computer attacks and effective defenses.* Upper Saddle River, N.J.; London: Prentice Hall PTR ; Pearson Education [distributor].

Smith, J. K. (1983). Quantitative versus interpretive: The problem of conducting social inquiry. *New Directions for Program Evaluation*, *1983*(19), 27–51.

Smith, K., & Hancock, P. (1995). Situation awareness is adaptive, externally directed consciousness. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 137–148.

Solansky, S. T., & Beck, T. E. (2009). Enhancing community safety and security through understanding interagency collaboration in cyber-terrorism exercises. *Administration & Society*, *40*(8), 852–875.

Somayaji, A., & Forrest, S. (2000). Automated response using system-call delays. In *Proceedings of the 9th USENIX Security Symposium* (Vol. 70).

Sommers, J., & Barford, P. (2004). Self-configuring network traffic generation. In *Proceedings of the 4th ACM SIGCOMM conference on Internet measurement* (pp. 68–81).

Soy, S. K. (1997). The case study as a research method. *Unpublished Paper, University of Texas at Austin*.

Spiegelberg, H. (1982). *The essentials of the phenomenological method*. Springer.

Squidoo. (2012). Definition and Types of Malware. *Squidoo*. Retrieved December 3, 2013, from http://www.squidoo.com/types-of-malware

Stanton, N. A., Chambers, P., & Piggott, J. (2001). Situational awareness and safety. *Safety Science*, *39*(3), 189–204.

Stebbins, R. A. (1997). Lifestyle as a generic concept in ethnographic research. *Quality and Quantity*, *31*(4), 347–360.

Stech, F. J., Heckman, K. E., Hilliard, P., & Ballo, J. R. (2011). Scientometrics of Deception, Counter-deception, and Deception Detection in Cyber-space. *PsychNology Journal*, *9*(2), 79–122.

Steiger, J. H. (1990). Structural model evaluation and modification: An interval estimation approach. *Multivariate Behavioral Research*, *25*(2), 173–180.

Stevens, J. (1996). Exploratory and confirmatory factor analysis. *Applied Multivariate Statistics for the Social Sciences*, 362–428.

Stevens, R. (2012). Federal Register, Volume 77 Issue 43 (Monday, March 5, 2012). *DHS Federal Register*, *77*(43), 13135–13136.

Stevens-Adams, S., Carbajal, A., Silva, A., Nauer, K., Anderson, B., Reed, T., & Forsythe, C. (2013). Enhanced Training for Cyber Situational Awareness. In *Foundations of Augmented Cognition* (pp. 90–99). Springer.

Stoil, R. ., & Goldstein, J. (2006, June 28). One if by land, two if by modem. *www.JPost.com*. Retrieved December 3, 2013, from http://www.jpost.com/Israel/One-if-by-land-two-if-by-modem

Strater, L. D., Endsley, M. R., Pleban, R. J., & Matthews, M. D. (2001). *Measures of platoon leader situation awareness in virtual decision-making exercises*. DTIC Document.

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation guidelines for IS positivist research. *Communications of the Association for Information Systems*, *13*(24), 380–427.

Straub, D. W., & Carlson, C. (1989). Validating instruments in MIS research. *MIS Quarterly*, 147–169.

Sudit, M., Stotz, A., & Holender, M. (2005). Situational awareness of a coordinated cyber attack. In *Defense and Security* (pp. 114–129). International Society for Optics and Photonics.

Sun Tzu, & Giles, L. (1994). *Sun Tzu on the Art of War: The Oldest Military Treatise in the World, Translated from the Chinese with Introduction and Critical Notes*. Luzac & Company.

Tabachnick, B. G. (2000). *Using multivariate statistics* (4th ed.). Boston, MA: Allyn and Bacon.

Tabachnick, B. G., & Fidell. (2007). *Using multivariate statistics*. Boston: Pearson/Allyn & Bacon.

Tadda, G. P. (2008). Measuring performance of Cyber situation awareness systems. In *2008 11th International Conference on Information Fusion* (pp. 1–8).

Tadda, G., Salerno, J. J., Boulware, D., Hinman, M., & Gorton, S. (2006). Realizing situation awareness within a cyber environment. In *Defense and Security Symposium* (pp. 624204–624204).

Tallinn Manual, & NATO Cooperative Cyber Defence Centre of Excellence. (2013). *Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. Cambridge ; New York: Cambridge University Press.

Taylor, R. (1990). Situational Awareness Rating Technique(SART): The development of a tool for aircrew systems design. *AGARD, Situational Awareness in Aerospace Operations 17 p(SEE N 90-28972 23-53)*.

The Economist. (2013, February 16). To the barricades. *The Economist*. Retrieved from http://www.economist.com/news/international/21571868-how-america-and-europe-are-trying-bolster-their-cyber-defences-barricades

The White House. (2009). Remarks by the President on Securing Our Nation's Cyber Infrastructure | The White House. Retrieved January 15, 2014, from http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure

Theohary, C. A., & Rollins, J. (2011). Terrorist Use of the Internet: Information Operations in Cyberspace.

Thomas, T.L. (2009). Taiwan Examines Chinese Information Warfare. *High Frontier, 5(3): 26-35*.

Tirenin, W., & Faatz, D. (1999). A concept for strategic cyber defense. In *Military Communications Conference Proceedings, 1999. MILCOM 1999. IEEE* (Vol. 1, pp. 458–463).

Tracy, M., Jansen, W., & McLarnon, M. (2009). Guidelines on Securing Public Web Servers. *NIST Special Publication*, *800*, 44.

TRADOC, U. (2010). Cyberspace Operations Concept Capability Plan 2016 2028. *Training and Doctrine Command (TRADOC) Pamphlet*, 525–7.

Tran, M. (2007, September 28). Internet access cut off in Burma. *the Guardian*. Retrieved December 3, 2013, from http://www.theguardian.com/world/2007/sep/28/burma.marktran

Tukey, J. W. (1977). Exploratory data analysis. *Reading, Ma*, *231*.

Vaishnavi, V., & Kuechler, B. (2009). DESRIST: Design Science Research in Information Systems Overview. Retrieved January 16, 2014, from http://desrist.org/desrist/

Van Creveld, M. L. (1987). *Command in war*. Harvard University Press.

Varon, E. (2002, January 15). SECURITY LEGISLATION - Homeland Defense: New Rules of War after 9/11. *CIO*. Retrieved December 3, 2013, from http://www.cio.com/article/30805/SECURITY_LEGISLATION_Homeland_Defense_New_Rules_of_War_after_9_11

Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model. *Information Systems Research*, *11*(4), 342–365.

Verton, D. (2002). The hacker diaries: confessions of teenage hackers.

Von Reibnitz, U. (1991). VON (1991): Szenario-Technik: Instrumente für die unternehmerische und persönliche Erfolgsplanung. *Gabler, Wiesbaden*.

Vreede, G. de. (1995). Facilitating organizational change. The participative application of dynamic modelling. *Delft University of Technology, Delft*.

Wagner, D. (2010). *White House sees no cyber attack on Wall Street*. Associated Press.

Wall, D. (2007). *Cybercrime: The transformation of crime in the information age* (Vol. 4). Polity.

Wang, W. (2006). *Steal this computer book 4.0: what they won't tell you about the Internet*. No Starch Press.

Whaley, B. (1982). Toward a general theory of deception. *The Journal of Strategic Studies*, *5*(1), 178–192.

Whaley, B., & Bell, J. B. (1991). *Cheating and deception*. Transaction Publishers New Brunswick.

White, B. (2003). *Dissertation Skills: For Business and Management Students*. Cengage Learning EMEA.

White House.gov. (2013). The Comprehensive National Cybersecurity Initiative | The White House. Retrieved January 15, 2014, from http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

Wickens, C. D. (2008). Situation awareness: Review of Mica Endsley's 1995 articles on situation awareness theory and measurement. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *50*(3), 397–403.

Winfield, I. (1991). *Organisations and information technology: systems, power and job design*. Oxford [England] ; Boston : Brookline Village, Mass: Blackwell ; Distributors, USA, Publishers' Business Services.

Wold, H. (1975). Modelling in complex situations with soft information. In *Third World Congress of Econometric Society* (pp. 21–26).

Wyler, N. R. (2005). *Aggressive network self-defense*. Access Online via Elsevier.

Yinn, R. (1984). *Case Study Research Design and Methods*. Beverly Hills, CA. Sage Publications.

Yuill, J., Denning, D. E., & Feer, F. (2006). *Using deception to hide things from hackers: Processes, principles, and techniques*. DTIC Document.

Zyda, M., Spraragen, M., & Ranganathan, B. (2009). Testing Behavioral Models with an Online Game. *IEEE Computer*, *42*(4), 103–105.

APPENDIX 1: EXPLORATORY SURVEY

1- SURVEY VARIABLES:

1.1 SA Variables:

Situational Awareness (SA)	S1	Perception Correctness	The extent to which awareness is consistent with ground truth
	S2	Perception Completeness	The percentage of relevant information attained
	S3	Previous Knowledge	The explicit knowledge which serves to formulate decisions and to generate new knowledge by fusing it with tacit knowledge
	S4	Skill	Ability to acquire new knowledge and the ability to convert both new and explicit knowledge into desired action
	S5	Analysis Capability	Systematically unravelling of the knowledge and understanding
	S6	Confidence	The willingness to use the information
	S7	Projection (intent)	The willingness to perform an act

1.2 Quality and Agility Variables:

Quality and Agility (QA)	ES1	Timeliness	The timeliness of awareness building
	ES2	Responsiveness	The ability to act within windows of opportunity
	ES3	Adaptability	The ability to adapt changes quickly
	ES4	Quality Accuracy	The quality of nearness to the truth, or the true value of the quality and usefulness of the knowledge provided
	ES5	Quality Reliability	The quality of the sources used to produce SA
	ES7	Quality Timeliness	The timeliness of intelligence

1.3 Intelligence Variables:

Intelligence Constructs			
1- Passive Intelligence (PI)	in1	Intelligence Timeliness	The timeliness of provided intelligence
	in2	Enemy IP	IP identification
	in3	Enemy Motive	The reason behind performing a given act
	in4	Passive Intelligence Gathering Capability	Local and public available intelligence (Sensors)
	in5	Intelligence Sharing	Intelligence provided and shared with partners
	in6	Intelligence Collaboration	Intelligence provided by partners
	in7	Interaction Capability	The capabilities to interact with enemy during a cyber incident
2- Active Intelligence (AI)	in8	Enemy Capabilities	Enemy strength and resources
	in9	Enemy Weaknesses	Enemy weak points that can be exploited
	in10	Intelligence Accuracy	The quality of information provided
	in11	Intelligence Completeness	The amount of truth captured
	in12	Information Gathering	The capacity to gather intelligence
	in13	Destroy	The capacity to eliminate threat offensively
	in14	Active Intelligence Gathering Capability	The capacity to actively gather intelligence from enemy domain
3- Intelligence Gathering	in15	Resources Availability	The resources available to extract intelligence
	in16	Non Cyber Intelligence	Intelligence that influences cyber operation
	in17	Enemy Geo Location	The geo-location of enemy
	in18	Enemy Attack Variation	Type of attacks that can be used against enemy
	in19	Enemy Attack Consistency	The strength of enemy attack
	in20	Granular level of Threat Detail	The known threat
	in21	Enemy Possible Attack	The possible attacks enemy can use against resources
	in22	Enemy Attack Timing	The duration of attack to be completed

Participant Information

Introduction

The purpose of this research is to explore the key factors associated with Cyber Situational Awareness and evaluate the strength of its association in order to build a comprehensive Active Cyber Situational Awareness.

ELIGIBILITY REQUIREMENTS:
To be eligible to take part in this study you must be part of the following:
1- IT Security
2- Network Security
3- Cyber Incident Response Team
4- Cyber Defence

TIME COMMITMENT:
This survey should only take about 15 minutes of your time. Your answers will be completely anonymous unless you decide to provide your personal details

PROCEDURE & PARTICIPANTS' RIGHTS:
The research will be conducted through a questionnaire survey where participation in this study is totally voluntary. Participants have the right to not take part of this survey or withdraw at any time prior to submitting the questionnaire. The survey result will be collected anonymously unless participants decide to provide their personal detail. All data collected will be kept confidential and used for the purposes of this research only. All your personal data will be kept secure and protected under the Data Protection Act 1998, no other entity will be granted to access this research data. Any publication that may be derived this survey will not include any sort of personal data.

Please note the survey is hosted by the USA based survey company Survey Monkey that is subject to US laws.Please visit the following address to understand your rights: https://www.surveymonkey.net/mp/policy/privacy-policy/

BENEFITS AND RISKS:
There are no known benefits or risks for participants in this study

FOR FURTHER INFORMATION:
If you have any questions at any time about the study, please do not hesitate to contact Ahmed Al-Shamisi (ahmed.al-shamisi@brunel.ac.uk)

Introduction

Dear All

Thank you very much for taking the time to complete this survey. Your feedback is important to us will enable us to build a strong Cyber Situational Awareness Model that can handle Cyber incidents and Enhance Cyber Commander's decision making process.

This survey should only take about 10 minutes of your time. Your answers will be completely anonymous.

1- How much do you agree or disagree with the given statement
(1- Do not agree 5- Strongly agree)

If you have any questions about the survey, please contact us at ahmed.al-shamisi@brunel.ac.uk.

In order to progress through this survey, please use the following navigation buttons:

Click the Next button to continue to the next page.
Click the Previous button to return to the previous page.
Click the Submit button to submit your survey.

Section 1: Intelligence

Intelligence gathering capabilities during a cyber incident is important for an organisation to handle enemy attacks.

Do not Agree 2 3 4 Strongly Agree

Collaboration and sharing intelligence across stakeholders and partners are required to enhance cyber Situational Awareness.

Do not Agree 2 3 4 Strongly Agree

Sharing intelligence resources and capabilities are required to build strong and reliable Cyber Situational Awareness.

Do Not Agree 2 3 4 Strongly Agree

Cyber collaboration is important to build strong and reliable Cyber Situational Awareness.

Do Not Agree 2 3 4 Strongly Agree

An Intelligence accuracy in cyberspace is vital in order to enhance Cyber Situational Awareness.

Do Not Agree 2 3 4 Strongly Agree

A good intelligence is one that has been provided in a timely manner and useful for an organization to enhance its Cyber Situational Awareness.

Do Not Agree 2 3 4 Strongly Agree

Completeness of cyber intelligence is required to enhance an organisation's Situational Awareness.

Do Not Agree 2 3 4 Strongly Agree

Combining other non cyber related sources of intelligence helps to enhance an organization Cyber Situational Awareness.

Do Not Agree 2 3 4 Strongly Agree

A granular level of threat detail helps to enhance organisation defence.

Do Not Agree 2 3 4 Strongly Agree

Resource availability helps to enhance cyber Situational Awareness.

Do Not Agree 2 3 4 Strongly Agree

1.1 Passive Data Collection

Security controls (IDS, Firewall, IPS, Anti-viruses) are a crucial source of intelligence that an organization has to enhance its Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

IP (Internet Protocol) identification is a key factor to build cyber Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

The attacker's geographical location helps an organization to enhance Cyber Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

Identifying the motive behind a cyber incident is vital for an organisation to build a strong Cyber Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

1.2 Active Data Collection

Active Situational Awareness through active intelligence gathering is required for future cyber security.

Do not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

The more interaction an organization has with the enemy, the more knowledge an organization can gather about the enemy.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

Information about the enemy's capabilities (Operating system, Services running, Tools used) enables a defending organization to evaluate the threat possibilities, which helps to enhance cyber Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

Identifying enemy weaknesses during a cyber incident helps an organisation to enhance Situational Awareness based on enemy vulnerabilities.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

Within an offensive approach, information about a possible attack which has an impact on enemy resources helps the defending organizations to enhance their Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

The defending organization with deception capabilities can enhance cyber Situational Awareness by deceiving an enemy to identify enemy attack timing.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

The defending organization with deception capabilities can enhance cyber Situational Awareness by deceiving an enemy to identify enemy attack consistency.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

The defending organization with deception capabilities can enhance cyber Situational Awareness by deceiving an enemy to identify all possible enemy attack variations.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

Within an offensive approach, a deceptive capability (Active intelligence Gathering) provides superior information that enhances cyber Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

Information about how to destroy an enemy in cyber space helps in enhancing the defending organization Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

Section 2: Situation Awareness

2.1: Perception

Perception of cyber incident is vital in building cyber Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

Understanding Cyber incident through comprehension is important to build cyber Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

Projecting enemies future course of action is vital to build cyber Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

Perceiving incorrect data leads to poor cyber Situational Awareness so training techniques and procedures employed by the defending organisation helps to avoid such an issue.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

Poor cyber Situational Awareness results from perceiving incomplete data so training techniques and procedures employed by the defending organisation helps to avoid such an issue.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

2.2: Comprehension

An organization that has rich and accessible previous information (such as vendor reports, previous cyber incident, Risk assessment reports, Cert report, etc.) allows an organization to build strong cyber Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

Comprehension of the cyber incident Situation is gained when an organisation relies on skilful and experienced employees.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

Cyber threat analysis is key to the comprehension of the cyber incident.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

Cyber Situational Awareness requires both willingness and trust to use cyber intelligence.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

2.3: Projection

Estimating the enemy's intent towards the defending organization's assets can enhance Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
○	○	○	○	○

Section 3: Enhanced Situational Awareness

3.1: Situational Awareness Agility

Agility is an important factor in cyber Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

The Situational Awareness is agile when Situational Awareness achieved in a timely manner.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

The Situational Awareness is agile when an organization has the capability to act within a window of opportunity during the cyber incident.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

The Situational Awareness is agile when an organization can adapt to changes quickly.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

3.2: Situational Awareness Quality

Information quality is an important factor in cyber Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

High quality Situatuional Awareness relies on accurate information.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

The reliability of the source is needed to produce high quality Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

High quality information provided in timely manner helps to enhance cyber Situational Awareness.

Do Not Agree	2	3	4	Strongly Agree
◯	◯	◯	◯	◯

Other Factors

Other Keys Factors not addressed in this survey that you believe ought to be considered for building strong Cyber Situational Awareness.

Statement 1:

Statement 1

Not Considered	2	3	4	Strongly Considered
○	○	○	○	○

Statement 1: Extent Addressed by your organization

Not Addressed	2	3	4	Totally Addressed
○	○	○	○	○

Statement 2:

Statement 2:

Not Considered	2	3	4	Strongly Considered
○	○	○	○	○

Statement 2: Extent Addressed by your organization

Not Addressed	2	3	4	Totally Addressed
○	○	○	○	○

APPENDIX 2: SEM SPSS ANALYSIS RESULT

1- MULTICOLLINEARITY

VIF greater than 10 is multicollinearity; during the test researcher found only 2 that might have multicollinearity issue, but not over 10. The rest are lower than 5, which is tolerable.

Coefficients[a]

Model		Collinearity Statistics	
		Tolerance	VIF
1	ES1	.377	2.653
	ES2	.304	3.286
	ES3	.240	4.172
	ES4	.363	2.752
	ES5	.343	2.915
	ES7	.381	2.623
	in2	.321	3.120
	in3	.358	2.792
	in4	.347	2.883
	in5	.261	3.837
	in6	.224	4.465
	in7	.495	2.021
	in8	.377	2.652
	in9	.225	4.453
	in10	.291	3.435
	in11	.238	4.195
	in12	.258	3.871
	in13	.241	4.155
	in14	.207	4.835
	in15	.382	2.619
	in16	.255	3.928
	in17	.223	4.477
	in18	.263	3.806
	in19	.273	3.667
	in20	.516	1.939
	in21	.630	1.587
	in22	.439	2.276
	S1	.274	3.648
	S2	.233	4.288
	S3	.165	6.057
	S4	.140	7.168
	S5	.264	3.786

	S6	.315	3.172
	S7	.408	2.452

2- CRONBACH'S ALPHA

Conduct and interpret an internal consistency reliability analysis through Cronbach's alpha, the corrected item-total correlations and the inter-item correlation matrix.

A- Agility and Quality

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	No. of Items
.903	.904	6

Above 0.7 so it is reliable

Item Statistics			
	Mean	Std. Deviation	No.
ES1	3.75	.764	271
ES2	3.84	.751	271
ES3	3.85	.764	271
ES4	3.71	.789	271
ES5	3.72	.728	271
ES7	3.80	.748	271

Item-Total Statistics					
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
ES1	18.91	10.125	.661	.462	.897
ES2	18.82	9.766	.766	.662	.882
ES3	18.81	9.442	.830	.729	.872
ES4	18.95	9.768	.717	.555	.889
ES5	18.94	9.915	.758	.611	.883
ES7	18.86	10.116	.682	.469	.894

No Deletion required for this scale

b- Intelligence

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	No. of Items
.925	.924	22

Item Statistics			
	Mean	Std. Deviation	No.
in1	2.74	.843	271
in2	2.85	.907	271
in3	2.72	.897	271
in4	3.04	.904	271
in5	3.00	.956	271
in6	3.01	.958	271
in7	2.89	.907	271
in8	3.45	.937	271
in9	3.45	.929	271
in10	3.52	.918	271
in11	3.72	.804	271
in12	3.37	.945	271
in13	3.64	.866	271
in14	3.71	.865	271
in15	2.38	.939	271
in16	2.32	.980	271
in17	2.18	.821	271
in18	2.20	.869	271
in19	2.22	.839	271
in20	3.90	.693	271
in21	3.20	.906	271
in22	3.91	.789	271

N21 should be deleted to get better Cronbacks

Item-Total Statistics					
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
in1	64.69	135.748	.579	.538	.921
in2	64.58	132.682	.686	.705	.919
in3	64.72	134.063	.625	.603	.921
in4	64.39	133.232	.661	.639	.920
in5	64.44	132.573	.652	.724	.920
in6	64.42	132.081	.674	.746	.920
in7	64.54	134.701	.585	.488	.921
in8	63.98	133.374	.628	.596	.920
in9	63.98	133.122	.646	.751	.920
in10	63.92	133.300	.646	.683	.920
in11	63.71	134.480	.681	.750	.920
in12	64.06	132.674	.656	.721	.920
in13	63.79	134.093	.648	.745	.920
in14	63.72	134.801	.612	.782	.921
in15	65.05	135.775	.511	.609	.923
in16	65.11	136.003	.476	.737	.924
in17	65.25	137.403	.507	.766	.923
in18	65.23	137.133	.489	.724	.923
in19	65.21	137.547	.487	.715	.923
in20	63.53	140.102	.443	.334	.924
in21	64.23	139.799	.337	.253	.926
in22	63.52	139.421	.419	.346	.924

c- Situational Awareness

Reliability Statistics		
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	No. of Items
.942	.942	7

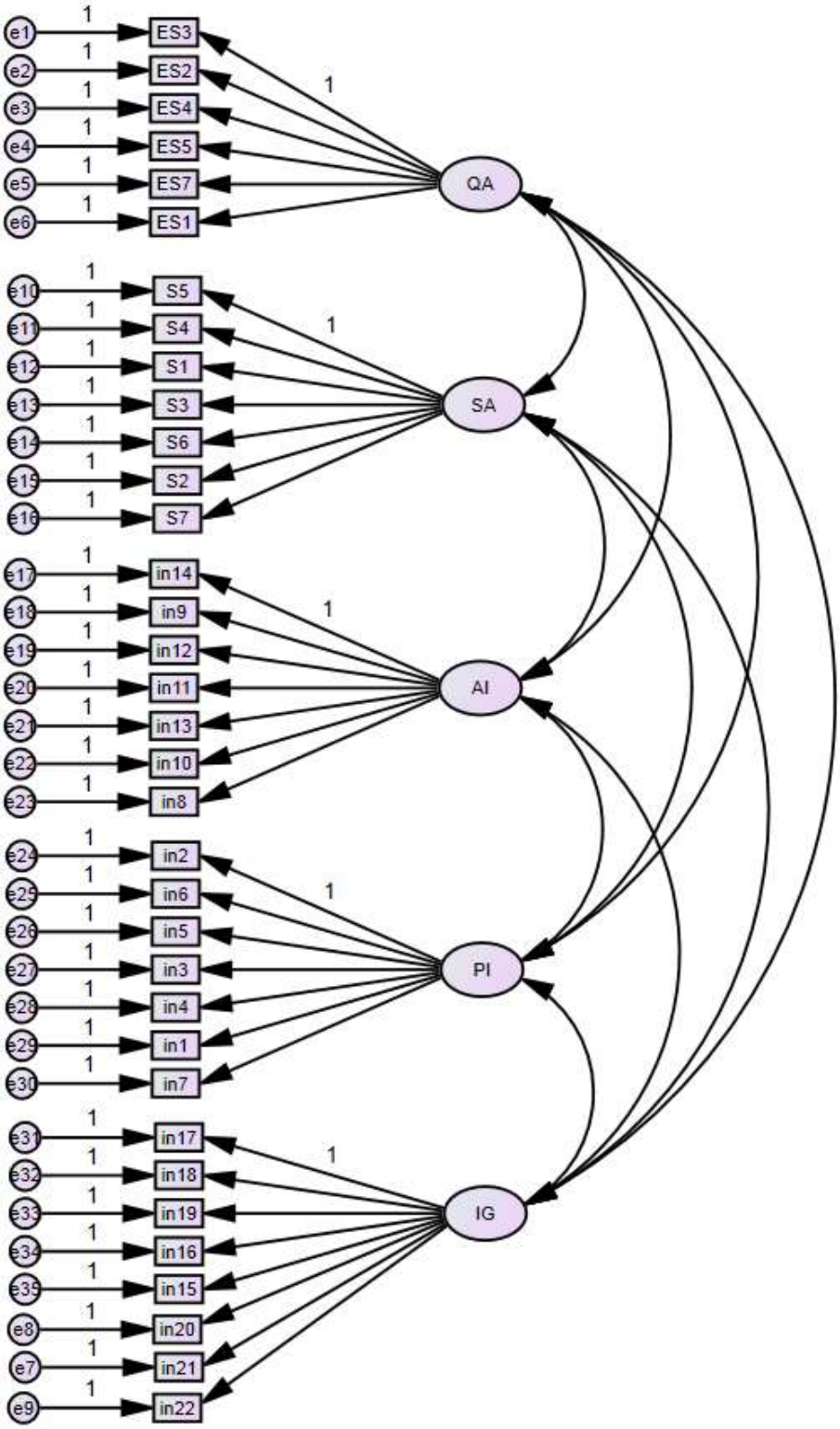
Item Statistics			
	Mean	Std. Deviation	No.
S1	4.04	.722	271
S2	4.00	.728	271
S3	3.99	.735	271
S4	3.98	.717	271
S5	4.05	.705	271
S6	4.07	.716	271
S7	4.11	.680	271

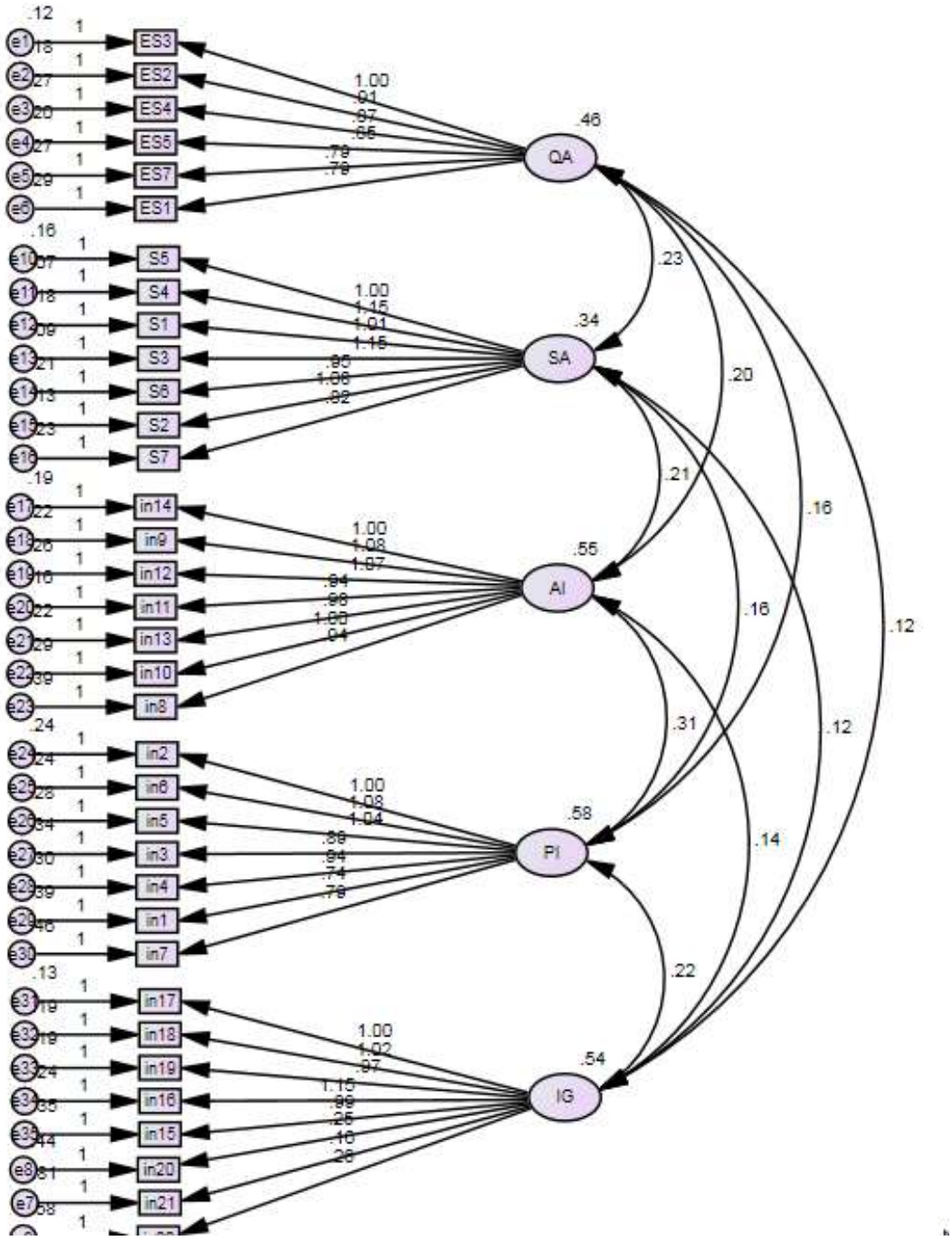
Item-Total Statistics					
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
S1	24.20	13.718	.812	.687	.933
S2	24.24	13.613	.826	.732	.931
S3	24.26	13.452	.850	.817	.929
S4	24.26	13.468	.873	.844	.927
S5	24.20	13.795	.818	.693	.932
S6	24.17	13.941	.771	.620	.936
S7	24.13	14.479	.703	.520	.942

3- CFA

Initial Model:

From previous analysis we found in20, in21,in22 could cause problems, so we watched them carefully.


e1
e2
e3
e4
e5
e6
ES3
ES2
ES4
ES5
ES7
ES1
QA
e10
e11
e12
e13
e14
e15
e16
S5
S4
S1
S3
S6
S2
S7
SA
e17
e18
e19
e20
e21
e22
e23
in14
in9
in12
in11
in13
in10
in8
AI
e24
e25
e26
e27
e28
e29
e30
in2
in6
in5
in3
in4
in1
in7
PI
e31
e32
e33
e34
e35
e8
e7
e9
in17
in18
in19
in16
in15
in20
in21
in22
IG
1



From visual inspection in 20,in21,in22 are loading very low

Standardized Residual Covariances (Group number 1 - Default model)

None of the above variables is within 2.5, so deletion of these variables is justifiable.

in20	<---	IG	.271
in21	<---	IG	.128
in22	<---	IG	.239

in22	-.975	-.498	.060	-.373	-.206	2.401	3.045	2.501	2.350	3.042
in20	.264	-.141	-.074	-.857	-.488	3.684	3.105	3.441	2.918	3.100
in21	.516	.056	-.592	-.892	-.409	2.325	3.753	2.880	4.201	3.599

The standardized residual covariance should be within |2.58| (Byrne, 2006). Factor loading (Standardized regression weight) should be greater than 0.5, and preferably above 0.7 (Byrne, 2006).

Result of initial model :

Model Fit Summary

CMIN

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	80	1491.791	550	.000	2.712
Saturated model	630	.000	0		
Independence model	35	8061.029	595	.000	13.548

RMR, GFI

Model	RMR	GFI	AGFI	PGFI
Default model	.075	.754	.719	.659
Saturated model	.000	1.000		
Independence model	.251	.174	.125	.164

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	.815	.800	.875	.864	.874
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

Parsimony-Adjusted Measures

Model	PRATIO	PNFI	PCFI
Default model	.924	.753	.808
Saturated model	.000	.000	.000
Independence model	1.000	.000	.000

NCP

Model	NCP	LO 90	HI 90
Default model	941.791	830.820	1060.396
Saturated model	.000	.000	.000
Independence model	7466.029	7179.401	7759.099

FMIN

Model	FMIN	F0	LO 90	HI 90
Default model	5.525	3.488	3.077	3.927
Saturated model	.000	.000	.000	.000
Independence model	29.856	27.652	26.590	28.737

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	.080	.075	.085	.000
Independence model	.216	.211	.220	.000

AIC

Model	AIC	BCC	BIC	CAIC
Default model	1651.791	1676.406	1939.960	2019.960
Saturated model	1260.000	1453.846	3529.335	4159.335
Independence model	8131.029	8141.799	8257.103	8292.103

ECVI

Model	ECVI	LO 90	HI 90	MECVI
Default model	6.118	5.707	6.557	6.209

Saturated model	4.667	4.667	4.667	5.385
Independence model	30.115	29.053	31.200	30.155

HOELTER

Model	HOELTER .05	HOELTER .01
Default model	110	115
Independence model	22	23

After fixing issues

Model Fit Summary

CMIN

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	88	689.324	440	.000	1.567
Saturated model	528	.000	0		
Independence model	32	7538.630	496	.000	15.199

RMR, GFI

Model	RMR	GFI	AGFI	PGFI
Default model	.030	.868	.842	.723
Saturated model	.000	1.000		
Independence model	.259	.181	.128	.170

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	.909	.897	.965	.960	.965
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

Parsimony-Adjusted Measures

Model	PRATIO	PNFI	PCFI
Default model	.887	.806	.856
Saturated model	.000	.000	.000
Independence model	1.000	.000	.000

NCP

Model	NCP	LO 90	HI 90
Default model	249.324	181.993	324.590
Saturated model	.000	.000	.000
Independence model	7042.630	6764.960	7326.724

FMIN

Model	FMIN	F0	LO 90	HI 90
Default model	2.553	.923	.674	1.202
Saturated model	.000	.000	.000	.000
Independence model	27.921	26.084	25.055	27.136

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	.046	.039	.052	.853
Independence model	.229	.225	.234	.000

AIC

Model	AIC	BCC	BIC	CAIC
Default model	865.324	889.831	1182.311	1270.311
Saturated model	1056.000	1203.038	2957.919	3485.919
Independence model	7602.630	7611.542	7717.898	7749.898

ECVI

Model	ECVI	LO 90	HI 90	MECVI
Default model	3.205	2.956	3.484	3.296

Saturated model	3.911	3.911	3.911	4.456
Independence model	28.158	27.129	29.210	28.191

HOELTER

Model	**HOELTER .05**	**HOELTER .01**
Default model	192	201
Independence model	20	21

Only problem is GFI AGFI but they are very close

CFA Validity

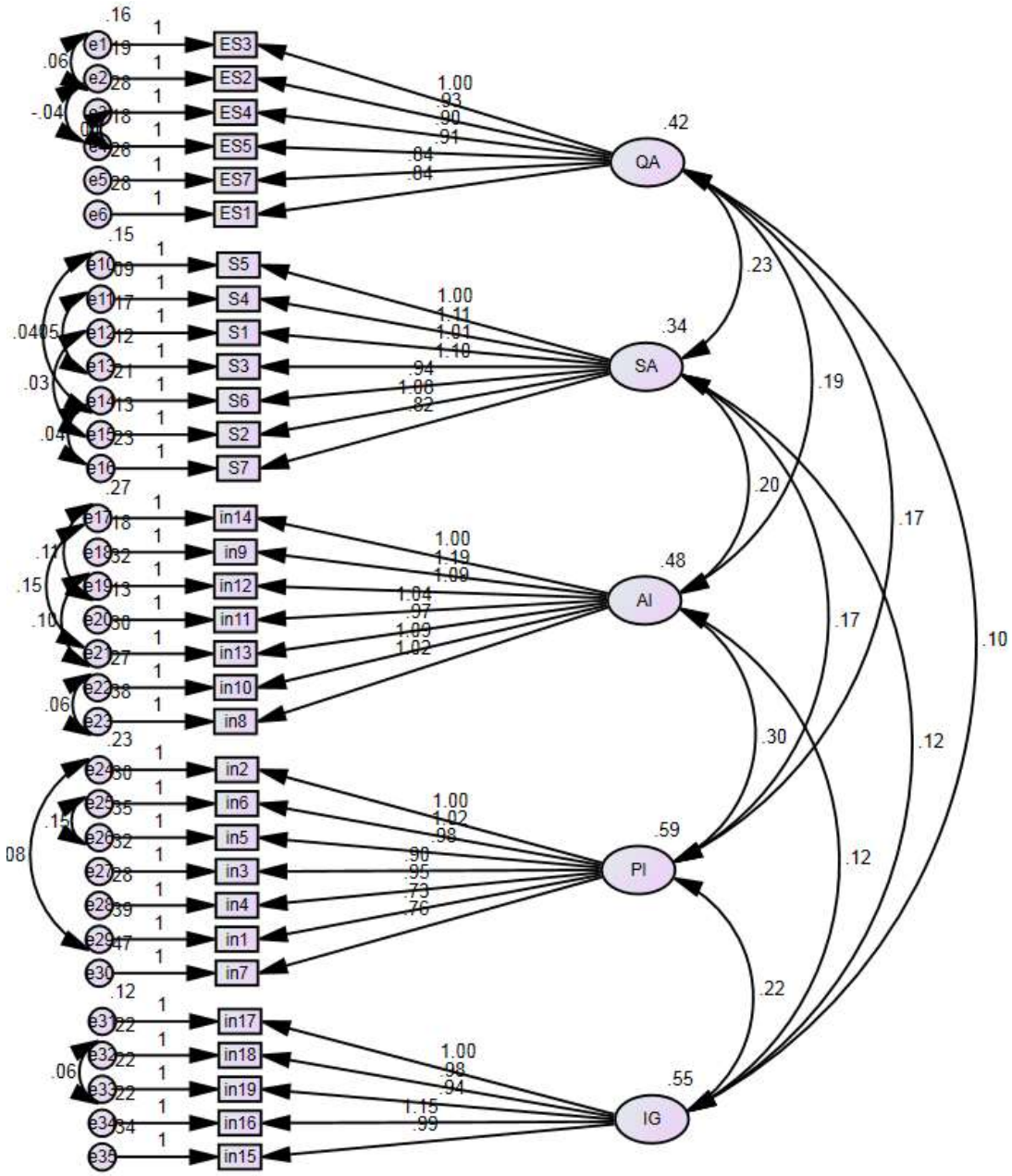
Correlations: (Group number 1 - Default model)					**Standardized Regression Weights: (Group number 1 - Default model)**			
			Estimate					Estimate
QA	<-->	SA	0.605		ES3	<---	QA	0.853
QA	<-->	AI	0.431		ES2	<---	QA	0.808
QA	<-->	PI	0.335		ES4	<---	QA	0.742
QA	<-->	IG	0.212		ES5	<---	QA	0.816
SA	<-->	AI	0.506		ES7	<---	QA	0.728
SA	<-->	PI	0.38		ES1	<---	QA	0.716
SA	<-->	IG	0.282		S5	<---	SA	0.83
AI	<-->	PI	0.565		S4	<---	SA	0.906
AI	<-->	IG	0.24		S1	<---	SA	0.819
PI	<-->	IG	0.39		S3	<---	SA	0.877
e25	<-->	e26	0.475		S6	<---	SA	0.768
e24	<-->	e29	0.279		S2	<---	SA	0.867
e17	<-->	e21	0.537		S7	<---	SA	0.71
e14	<-->	e16	0.183		in14	<---	AI	0.8
e12	<-->	e15	0.228		in9	<---	AI	0.887
e11	<-->	e13	0.477		in12	<---	AI	0.801
e3	<-->	e4	0.2		in11	<---	AI	0.892
e2	<-->	e4	-0.231		in13	<---	AI	0.777
e1	<-->	e2	0.325		in10	<---	AI	0.82
e32	<-->	e33	0.277		in8	<---	AI	0.751
e22	<-->	e23	0.192		in2	<---	PI	0.85
e17	<-->	e19	0.361		in6	<---	PI	0.819
e10	<-->	e14	0.234		in5	<---	PI	0.786

e19	<-->	e21	0.327		in3	<---	PI	0.777
					in4	<---	PI	0.809
					in1	<---	PI	0.667
					in7	<---	PI	0.649
					in17	<---	IG	0.906
					in18	<---	IG	0.841
					in19	<---	IG	0.831
					in16	<---	IG	0.877
					in15	<---	IG	0.782

	CR	AVE	MSV	ASV	PI	QA	SA	AI	IG
PI	0.909	0.591	0.319	0.182	0.769				
QA	0.902	0.607	0.366	0.177	0.335	0.779			
SA	0.938	0.685	0.366	0.211	0.380	0.605	0.828		
AI	0.935	0.672	0.319	0.205	0.565	0.431	0.506	0.820	
IG	0.928	0.720	0.152	0.084	0.390	0.212	0.282	0.240	0.848

No Validity Concerns

4- FINAL CFA


QA
SA
AI
PI
IG
ES3
ES2
ES4
ES5
ES7
ES1
S5
S4
S1
S3
S6
S2
S7
in14
in9
in12
in11
in13
in10
in8
in2
in6
in5
in3
in4
in1
in7
in17
in18
in19
in16
in15
.42
.34
.48
.59
.55
.23
.19
.20
.17
.17
.10
.30
.12
.12
.22

5- SEM INITIAL TESTS:

Linearity Test

From curve estimation we found all relation are sufficiently linear.

DV: QA – IV: SA

Model Summary and Parameter Estimates

Dependent Variable: QA

Equation	Model Summary					Parameter Estimates			
	R Square	F	df1	df2	Sig.	Constant	b1	b2	b3
Linear	.419	193.614	1	269	.000	1.272	.697		
Logarithmic	.400	179.617	1	269	.000	.852	2.322		
Inverse	.345	141.505	1	269	.000	5.727	-6.663		
Quadratic	.419	96.489	2	268	.000	1.418	.613	.012	
Cubic	.427	66.404	3	267	.000	5.225	-3.071	1.139	-.110
Compound	.399	178.365	1	269	.000	1.847	1.214		
Power	.389	171.518	1	269	.000	1.628	.654		
S	.342	139.756	1	269	.000	1.866	-1.896		
Growth	.399	178.365	1	269	.000	.613	.194		
Exponential	.399	178.365	1	269	.000	1.847	.194		
Logistic	.399	178.365	1	269	.000	.542	.823		

The independent variable is SA.

DV: QA - IV: AI

Model Summary and Parameter Estimates

Dependent Variable: QA

Equation	Model Summary					Parameter Estimates			
	R Square	F	df1	df2	Sig.	Constant	b1	b2	b3
Linear	.216	74.031	1	269	.000	2.532	.416		
Logarithmic	.199	66.981	1	269	.000	2.538	1.173		
Inverse	.157	50.249	1	269	.000	4.762	-2.645		
Quadratic	.217	37.035	2	268	.000	2.758	.267	.023	
Cubic	.221	25.232	3	267	.000	4.107	-1.209	.524	-.054
Compound	.197	65.832	1	269	.000	2.646	1.120		
Power	.184	60.474	1	269	.000	2.645	.321		
S	.146	45.868	1	269	.000	1.583	-.727		
Growth	.197	65.832	1	269	.000	.973	.113		
Exponential	.197	65.832	1	269	.000	2.646	.113		
Logistic	.197	65.832	1	269	.000	.378	.893		

The independent variable is AI.

DV: QA – IV: PI

Model Summary and Parameter Estimates

Dependent Variable: QA

Equation	Model Summary					Parameter Estimates			
	R Square	F	df1	df2	Sig.	Constant	b1	b2	b3
Linear	.135	41.999	1	269	.000	2.983	.310		
Logarithmic	.128	39.631	1	269	.000	3.021	.838		
Inverse	.113	34.101	1	269	.000	4.601	-1.912		
Quadratic	.136	21.069	2	268	.000	3.190	.164	.024	
Cubic	.138	14.214	3	267	.000	2.515	.909	-.232	.028
Compound	.138	42.991	1	269	.000	2.948	1.094		
Power	.139	43.576	1	269	.000	2.957	.249		
S	.132	40.806	1	269	.000	1.562	-.591		
Growth	.138	42.991	1	269	.000	1.081	.089		
Exponential	.138	42.991	1	269	.000	2.948	.089		
Logistic	.138	42.991	1	269	.000	.339	.914		

The independent variable is PI.

DV: QA – IV: IG

Model Summary and Parameter Estimates

Dependent Variable: QA

Equation	Model Summary					Parameter Estimates			
	R Square	F	df1	df2	Sig.	Constant	b1	b2	b3
Linear	.053	15.133	1	269	.000	3.496	.200		
Logarithmic	.053	15.204	1	269	.000	3.623	.427		
Inverse	.049	13.928	1	269	.000	4.307	-.732		
Quadratic	.053	7.560	2	268	.001	3.443	.248	-.010	
Cubic	.060	5.642	3	267	.001	2.760	1.246	-.448	.058
Compound	.055	15.667	1	269	.000	3.415	1.060		
Power	.058	16.547	1	269	.000	3.537	.127		
S	.056	15.844	1	269	.000	1.469	-.222		
Growth	.055	15.667	1	269	.000	1.228	.058		
Exponential	.055	15.667	1	269	.000	3.415	.058		
Logistic	.055	15.667	1	269	.000	.293	.943		

The independent variable is IG.

DV: SA- IV: AI

Model Summary and Parameter Estimates

Dependent Variable: SA

Equation	Model Summary					Parameter Estimates			
	R Square	F	df1	df2	Sig.	Constant	b1	b2	b3
Linear	.283	106.325	1	269	.000	2.325	.443		
Logarithmic	.284	106.952	1	269	.000	2.269	1.300		
Inverse	.259	94.025	1	269	.000	4.804	-3.150		
Quadratic	.285	53.410	2	268	.000	2.003	.656	-.033	
Cubic	.291	36.453	3	267	.000	.583	2.209	-.560	.056
Compound	.285	107.381	1	269	.000	2.428	1.139		
Power	.297	113.907	1	269	.000	2.368	.390		
S	.282	105.712	1	269	.000	1.629	-.965		
Growth	.285	107.381	1	269	.000	.887	.130		
Exponential	.285	107.381	1	269	.000	2.428	.130		
Logistic	.285	107.381	1	269	.000	.412	.878		

The independent variable is AI.

DV: SA- IV: PI

Model Summary and Parameter Estimates

Dependent Variable: SA

Equation	Model Summary					Parameter Estimates			
	R Square	F	df1	df2	Sig.	Constant	b1	b2	b3
Linear	.165	53.105	1	269	.000	2.842	.318		
Logarithmic	.164	52.635	1	269	.000	2.861	.878		
Inverse	.150	47.538	1	269	.000	4.533	-2.051		
Quadratic	.165	26.507	2	268	.000	2.730	.397	-.013	
Cubic	.167	17.849	3	267	.000	2.094	1.099	-.255	.026
Compound	.160	51.147	1	269	.000	2.843	1.096		
Power	.163	52.390	1	269	.000	2.847	.257		
S	.154	49.000	1	269	.000	1.539	-.610		
Growth	.160	51.147	1	269	.000	1.045	.092		
Exponential	.160	51.147	1	269	.000	2.843	.092		
Logistic	.160	51.147	1	269	.000	.352	.912		

The independent variable is PI.

DV: SA –IV: IG

Model Summary and Parameter Estimates

Dependent Variable: SA

Equation	Model Summary					Parameter Estimates			
	R Square	F	df1	df2	Sig.	Constant	b1	b2	b3
Linear	.088	26.048	1	269	.000	3.294	.239		
Logarithmic	.089	26.203	1	269	.000	3.446	.511		
Inverse	.083	24.189	1	269	.000	4.267	-.879		
Quadratic	.089	13.014	2	268	.000	3.232	.296	-.012	
Cubic	.096	9.495	3	267	.000	2.517	1.340	-.470	.061
Compound	.090	26.614	1	269	.000	3.227	1.074		
Power	.095	28.139	1	269	.000	3.368	.155		
S	.091	27.041	1	269	.000	1.466	-.272		
Growth	.090	26.614	1	269	.000	1.172	.071		
Exponential	.090	26.614	1	269	.000	3.227	.071		
Logistic	.090	26.614	1	269	.000	.310	.931		

The independent variable is IG.

DV: AI –IV: PI

Model Summary and Parameter Estimates

Dependent Variable: AI

Equation	Model Summary					Parameter Estimates			
	R Square	F	df1	df2	Sig.	Constant	b1	b2	b3
Linear	.370	157.710	1	269	.000	1.610	.573		
Logarithmic	.358	150.166	1	269	.000	1.664	1.562		
Inverse	.315	123.782	1	269	.000	4.612	-3.573		
Quadratic	.370	78.582	2	268	.000	1.547	.617	-.007	
Cubic	.370	52.202	3	267	.000	1.434	.742	-.050	.005
Compound	.352	146.002	1	269	.000	1.831	1.210		
Power	.360	151.154	1	269	.000	1.836	.534		
S	.338	137.243	1	269	.000	1.629	-1.262		
Growth	.352	146.002	1	269	.000	.605	.191		
Exponential	.352	146.002	1	269	.000	1.831	.191		
Logistic	.352	146.002	1	269	.000	.546	.826		

The independent variable is PI.

DV: AI –IV: IG

Model Summary and Parameter Estimates

Dependent Variable: AI

Equation	Model Summary					Parameter Estimates			
	R Square	F	df1	df2	Sig.	Constant	b1	b2	b3
Linear	.065	18.851	1	269	.000	2.818	.248		
Logarithmic	.069	19.911	1	269	.000	2.967	.541		
Inverse	.065	18.837	1	269	.000	3.841	-.942		
Quadratic	.068	9.834	2	268	.000	2.557	.485	-.049	
Cubic	.069	6.573	3	267	.000	2.362	.770	-.174	.017
Compound	.064	18.402	1	269	.000	2.730	1.087		
Power	.071	20.663	1	269	.000	2.860	.188		
S	.071	20.663	1	269	.000	1.359	-.335		
Growth	.064	18.402	1	269	.000	1.004	.084		
Exponential	.064	18.402	1	269	.000	2.730	.084		
Logistic	.064	18.402	1	269	.000	.366	.920		

The independent variable is IG.

Multicollinearity

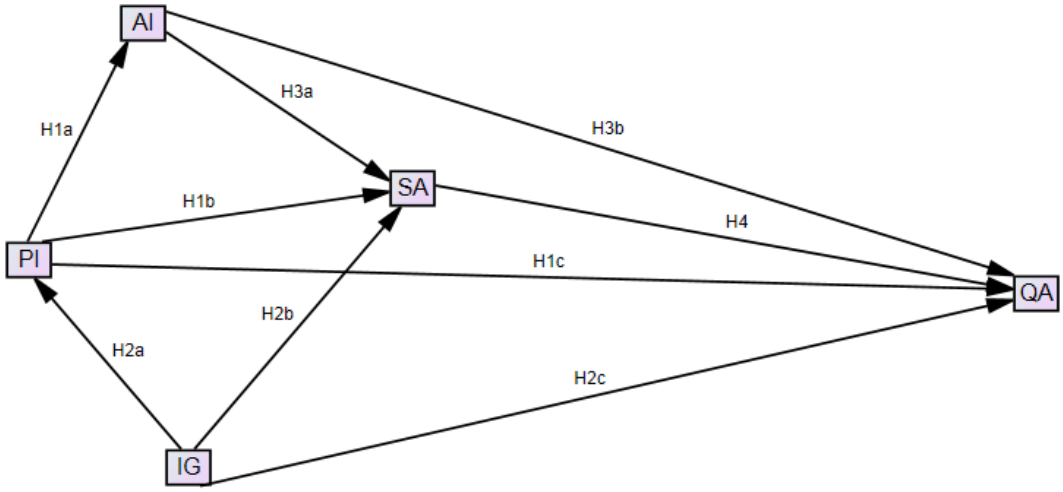
No issues

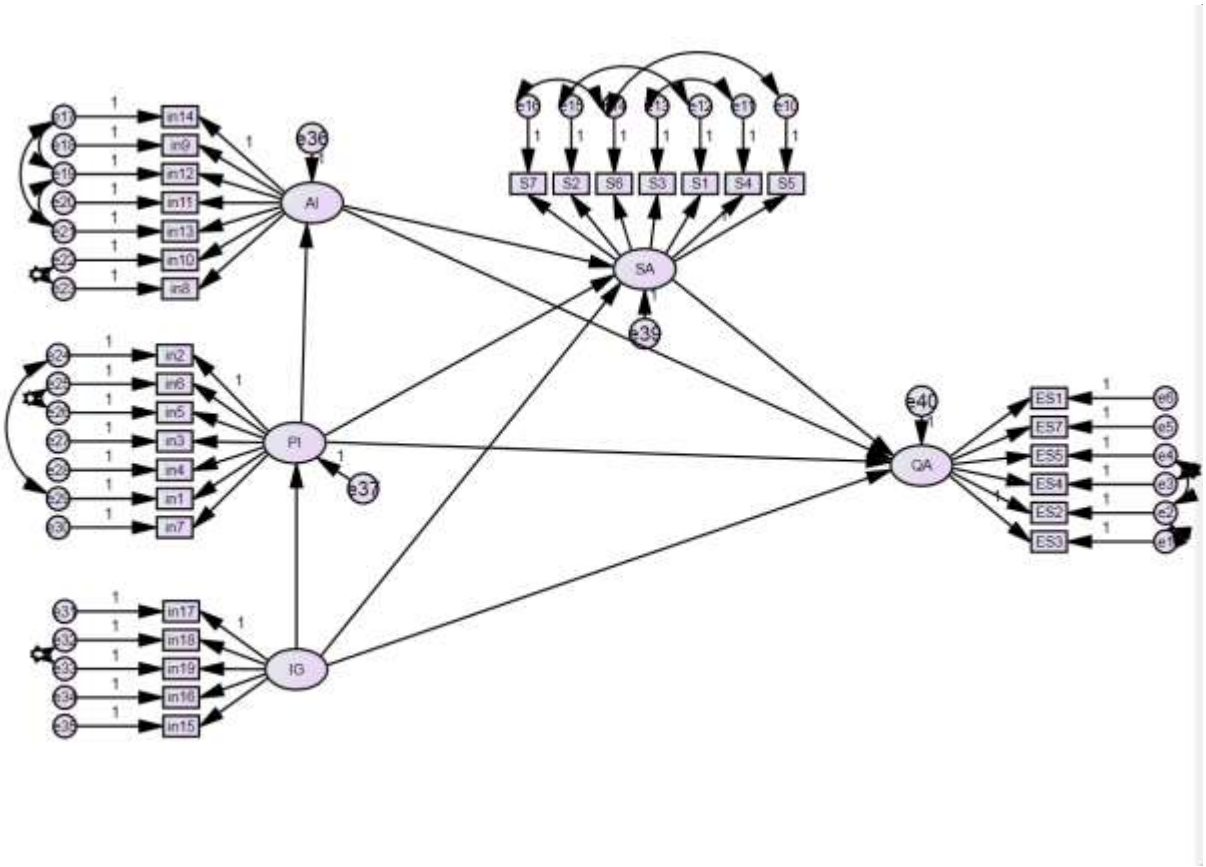
Coefficients[a]

Model		Collinearity Statistics	
		Tolerance	VIF
1	IG	.802	1.247
	PI	.554	1.804
	AI	.531	1.884
	SA	.687	1.457

a. Dependent Variable: QA

6- SEM INITIAL MODEL:





Result: Three highlighted regressions shows non-significant

Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
PI	<---	IG	.405	.066	6.093	***	
AI	<---	PI	.509	.059	8.642	***	
SA	<---	AI	.359	.064	5.601	***	
SA	<---	PI	.063	.059	1.067	.286	
SA	<---	IG	.117	.049	2.367	.018	
QA	<---	SA	.568	.079	7.146	***	
QA	<---	AI	.128	.071	1.803	.071	
QA	<---	IG	.011	.053	.204	.838	
QA	<---	PI	.050	.063	.787	.431	

Model Fit Summary

CMIN

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	87	689.461	441	.000	1.563
Saturated model	528	.000	0		
Independence model	32	7538.630	496	.000	15.199

RMR, GFI

Model	RMR	GFI	AGFI	PGFI
Default model	.030	.868	.842	.725
Saturated model	.000	1.000		
Independence model	.259	.181	.128	.170

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	.909	.897	.965	.960	.965
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

Parsimony-Adjusted Measures

Model	PRATIO	PNFI	PCFI
Default model	.889	.808	.858
Saturated model	.000	.000	.000
Independence model	1.000	.000	.000

NCP

Model	NCP	LO 90	HI 90
Default model	248.461	181.158	323.700
Saturated model	.000	.000	.000
Independence model	7042.630	6764.960	7326.724

FMIN

Model	FMIN	F0	LO 90	HI 90
Default model	2.554	.920	.671	1.199
Saturated model	.000	.000	.000	.000
Independence model	27.921	26.084	25.055	27.136

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	.046	.039	.052	.861
Independence model	.229	.225	.234	.000

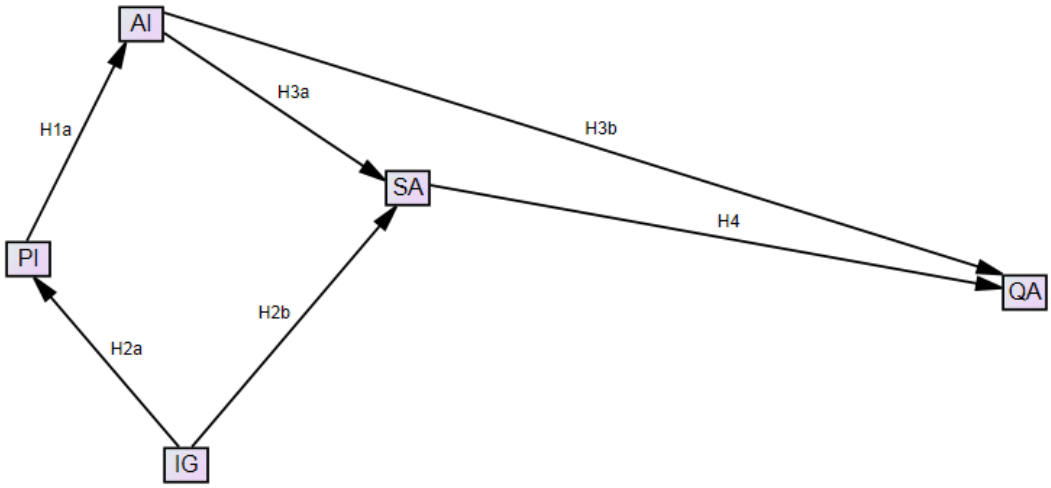
AIC

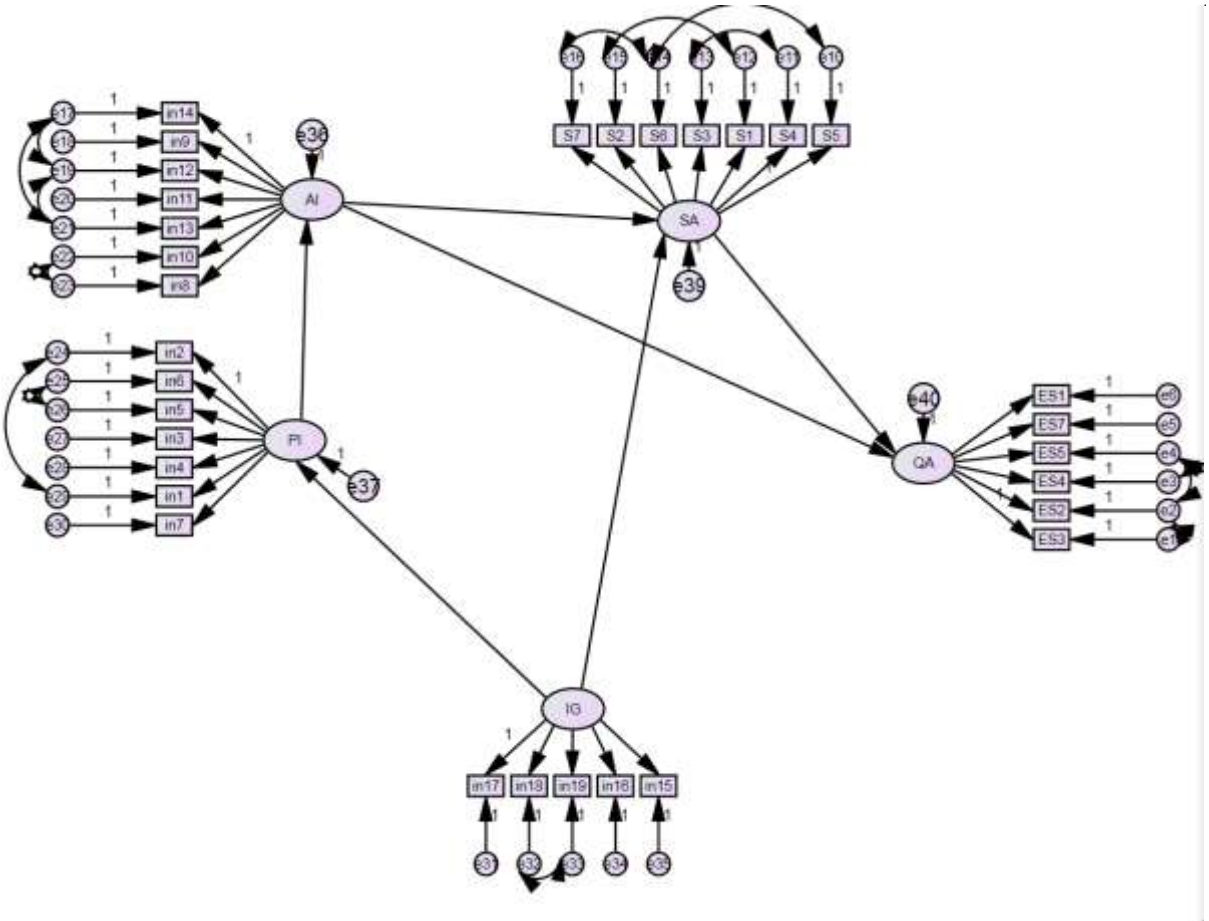
Model	AIC	BCC	BIC	CAIC
Default model	863.461	887.688	1176.845	1263.845
Saturated model	1056.000	1203.038	2957.919	3485.919
Independence model	7602.630	7611.542	7717.898	7749.898

ECVI

Model	ECVI	LO 90	HI 90	MECVI
Default model	3.198	2.949	3.477	3.288
Saturated model	3.911	3.911	3.911	4.456
Independence model	28.158	27.129	29.210	28.191

7- FINAL SEM


AI
H1a
H3a
H3b
SA
H4
PI
QA
H2b
H2a
IG


AI
SA
PI
QA
IG
S7
S2
S6
S3
S1
S4
S5
ES1
ES7
ES5
ES4
ES2
ES3
in17
in18
in19
in16
in15

Result:

Regression Weights: (Group number 1 - Default model)

			Estimate	S.E.	C.R.	P	Label
PI	<---	IG	.406	.066	6.104	***	
AI	<---	PI	.512	.059	8.694	***	
SA	<---	AI	.396	.055	7.229	***	
SA	<---	IG	.136	.046	2.940	.003	
QA	<---	SA	.578	.078	7.367	***	
QA	<---	AI	.160	.062	2.594	.009	

All Significant

Model Fit Summary

CMIN

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	84	691.547	444	.000	1.558
Saturated model	528	.000	0		
Independence model	32	7538.630	496	.000	15.199

RMR, GFI

Model	RMR	GFI	AGFI	PGFI
Default model	.032	.868	.843	.730
Saturated model	.000	1.000		
Independence model	.259	.181	.128	.170

Baseline Comparisons

Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	.908	.898	.965	.961	.965
Saturated model	1.000		1.000		1.000
Independence model	.000	.000	.000	.000	.000

Parsimony-Adjusted Measures

Model	PRATIO	PNFI	PCFI
Default model	.895	.813	.864
Saturated model	.000	.000	.000
Independence model	1.000	.000	.000

NCP

Model	NCP	LO 90	HI 90
Default model	247.547	180.201	322.833
Saturated model	.000	.000	.000
Independence model	7042.630	6764.960	7326.724

FMIN

Model	FMIN	F0	LO 90	HI 90
Default model	2.561	.917	.667	1.196
Saturated model	.000	.000	.000	.000
Independence model	27.921	26.084	25.055	27.136

RMSEA

Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	.045	.039	.052	.875
Independence model	.229	.225	.234	.000

AIC

Model	AIC	BCC	BIC	CAIC
Default model	859.547	882.940	1162.125	1246.125
Saturated model	1056.000	1203.038	2957.919	3485.919
Independence model	7602.630	7611.542	7717.898	7749.898

ECVI

Model	ECVI	LO 90	HI 90	MECVI
Default model	3.184	2.934	3.462	3.270
Saturated model	3.911	3.911	3.911	4.456
Independence model	28.158	27.129	29.210	28.191

HOELTER

Model	HOELTER .05	HOELTER .01
Default model	193	202
Independence model	20	21

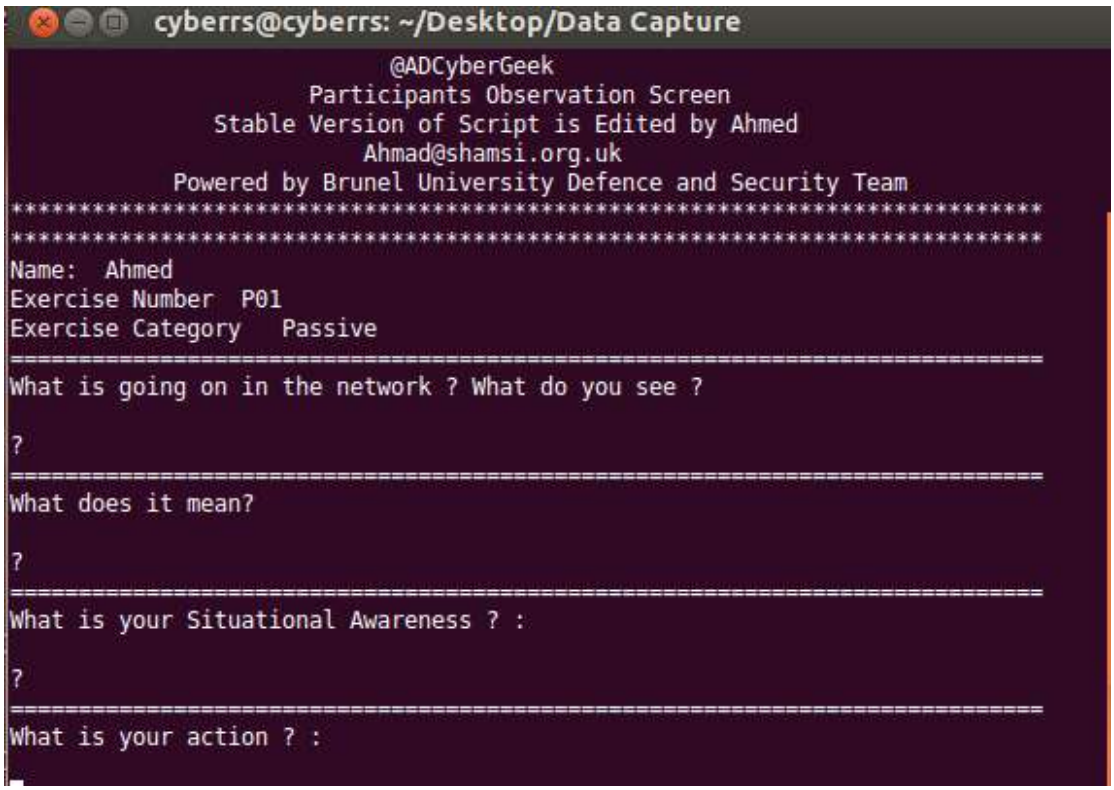
APPENDIX 3: LAB EXPERIMENT SESSION:

1- EXPERIMENT ENVIRONMENT:

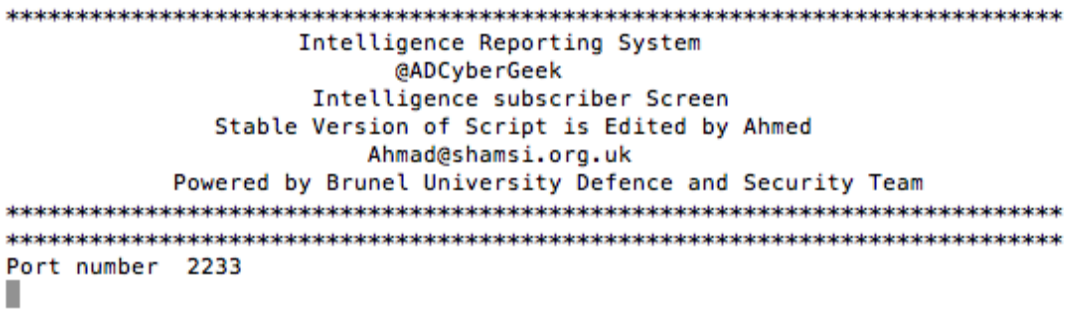
2- EXPERIMENT ENVIRONMENTS TOOLS

2.1 Coded Tools:

a- Data capture tool:



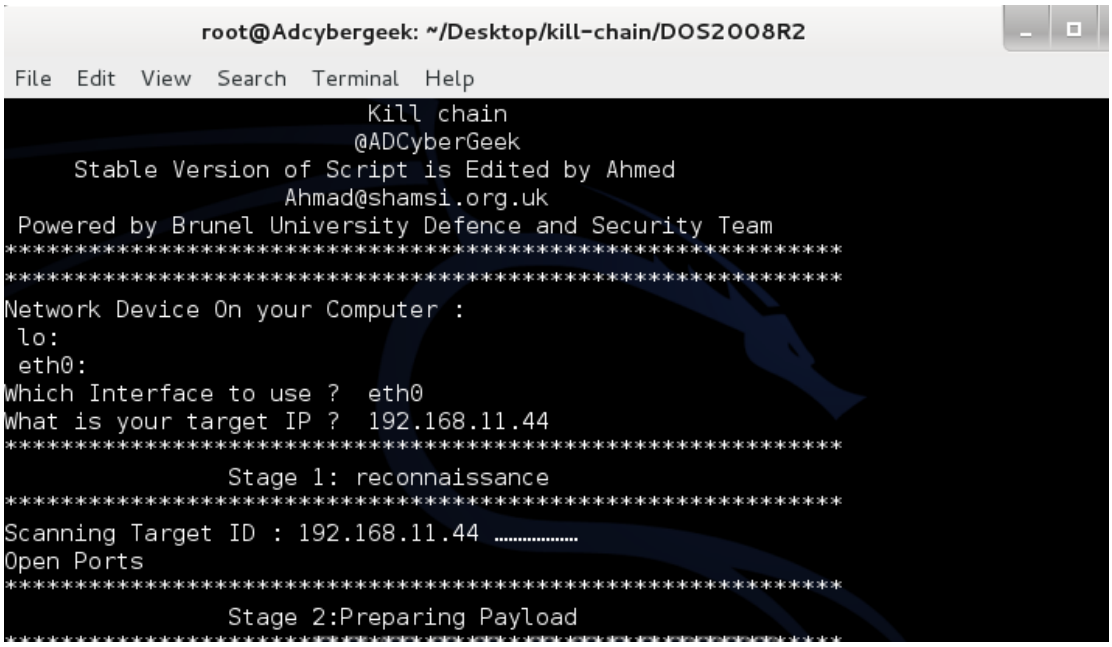
b- Intelligence reporting tool:



c- Server-side intelligence reporting system code:

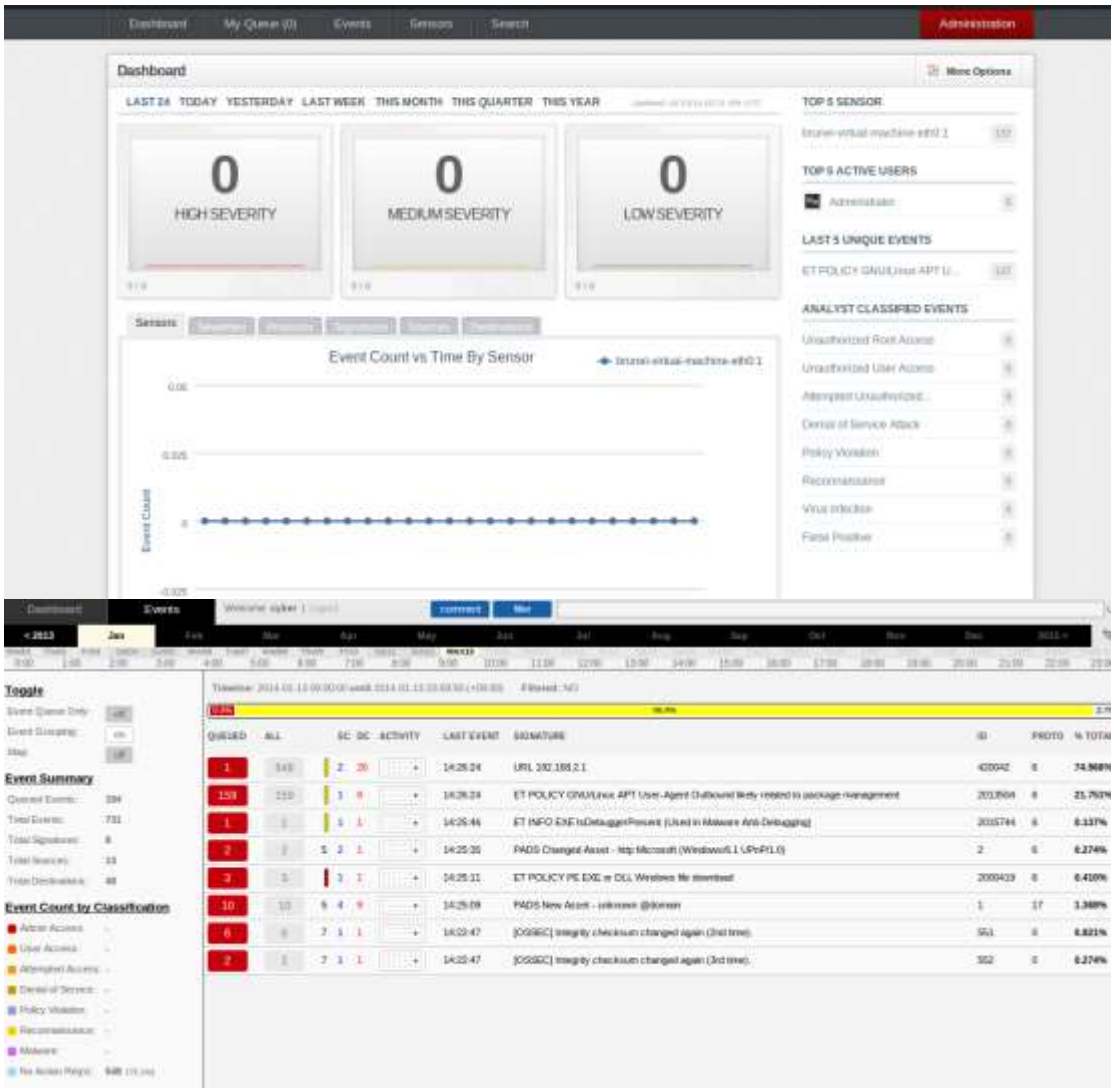
```
#!/bin/bash

clear
echo "*********************************************************************************"
echo "                     Intelligence Reporting System        "
echo "                           @ADCyberGeek        "
echo "                      Intelligence Reporting Screen        "
echo "               Stable Version of Script is Edited by Ahmed  "
echo "                           Ahmad@shamsi.org.uk           "
echo "            Powered by Brunel University Defence and Security Team           "
echo "*********************************************************************************"
echo "*********************************************************************************"
echo -e "Subscriber IP:  \c"
read Sip
echo -e "Subscriber Port  \c"
read Sport
for (( ; ; ))
do
echo -e "Intelligence Reference Number:  \c"
read intlref
echo -e "Intelligence Priority:  \c"
read pri
echo -e "Intelligence Description :  \c"
read dis
NOW=$(date +"%c")
echo "*********************************************************************************" >>
test.txt
echo "**************************** $NOW ***********************" >> test.txt
echo "*********************************************************************************" >>
```

d- Kill-chain automated script:

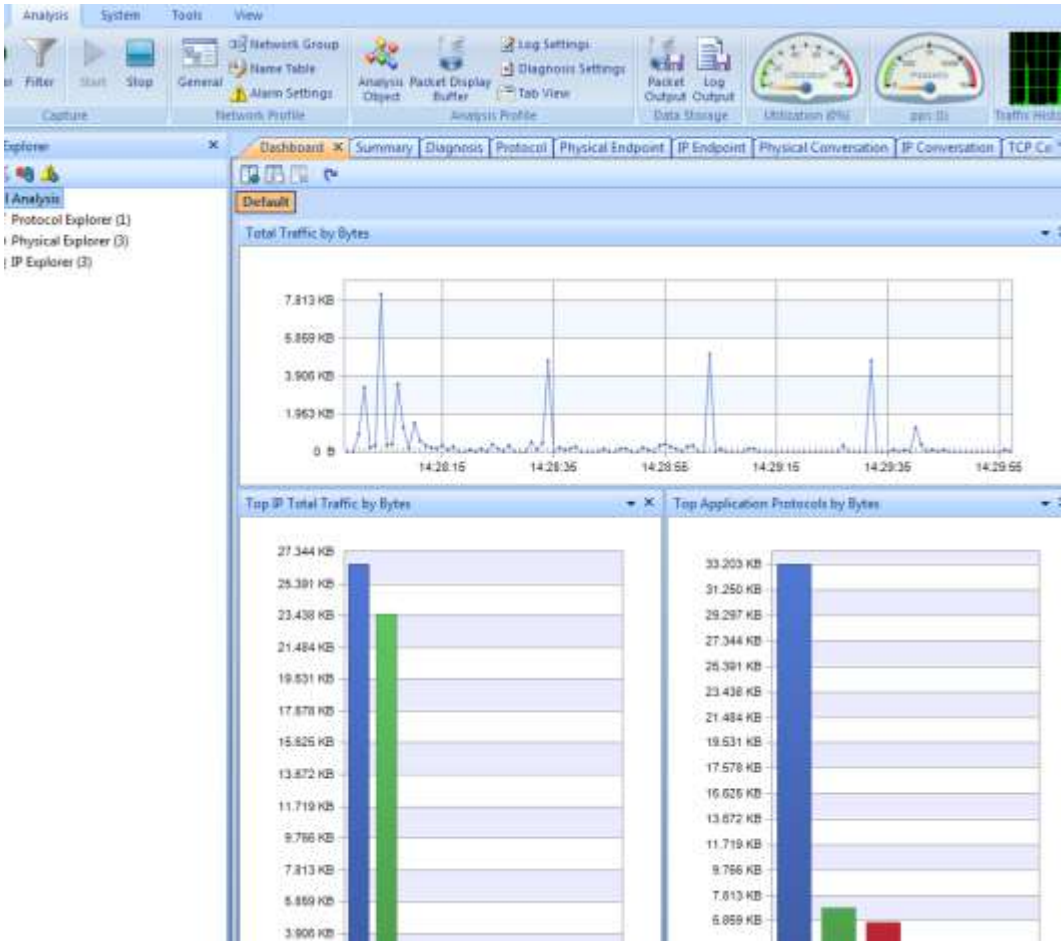


2.2- Networking and Alerts Tools

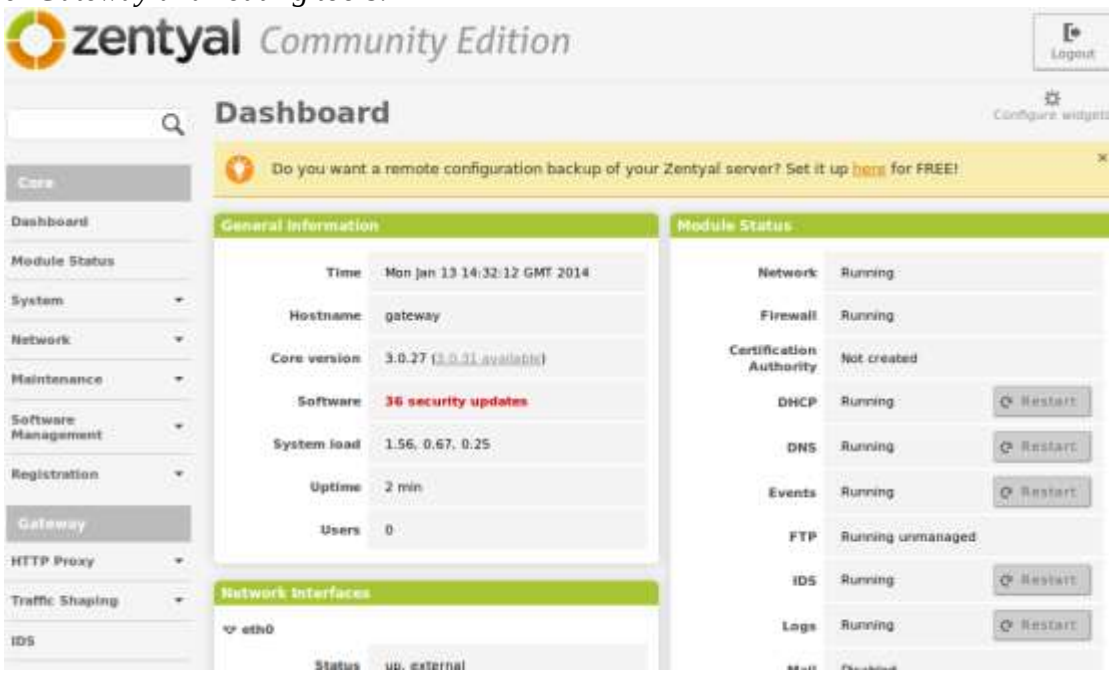
a- IDS:



b- Network monitoring tools:



c- Gateway and routing tools:



2.3- Experiment Exercises

a. Exercise one: (controlled group)

You have been asked to monitor an ADX system and make sure you keep it safe and available. The tools you have for this exercise are:

1. Network Activities Monitoring Solution.
2. Intrusion Detection System.
3. Live intrusion Detection Alert System.
4. Firewall.

During the exercise, participants should speak out loud whenever they come to a point of perception or decisions. As explained in the induction session, participants will be asked to fill out answers to several questions during the experiment, and they may ask at any point to freeze the exercise.

b. Exercise Two: (experimental group)

You have been asked to monitor an ADX system and make sure you keep it safe and available. The tools you have for this exercise are:

1- Network Activities Monitoring Solution.
2- Intrusion Detection System.
3- Live intrusion Detection Alert System.
4- Firewall.
5- Intelligence Reporting System.
6- Blue Team (with offensive capabilities).
7- Deception Services.

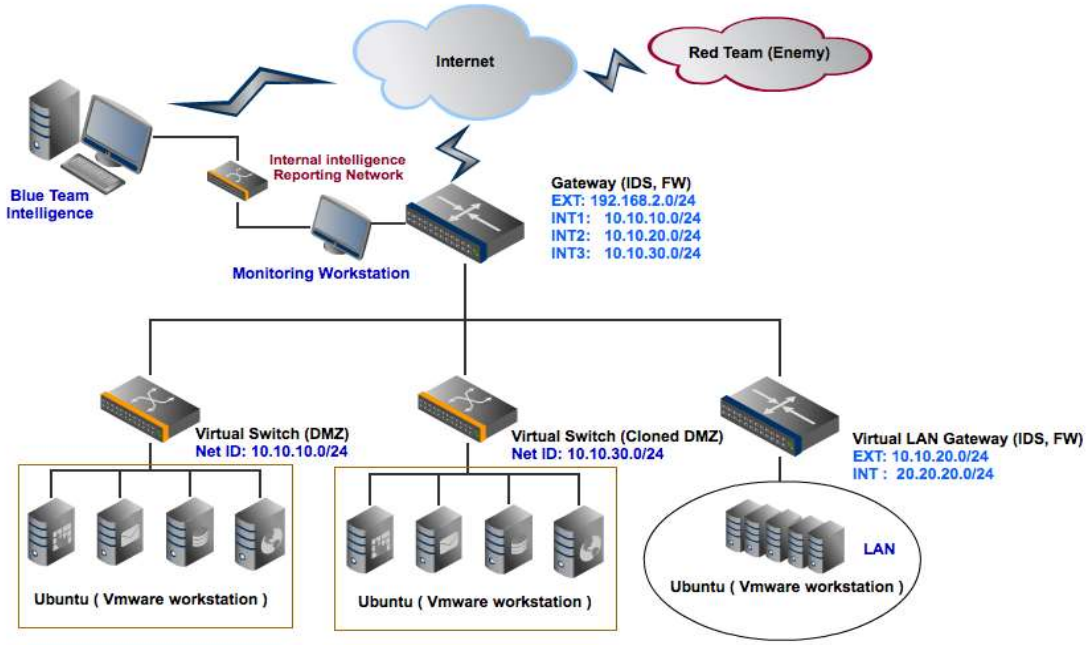
During the exercise, participants should speak loud whenever they come to a point of perception or decisions. Also, participants may use deception services to buy extra time or to collect intelligence about attackers in a safe and controlled environment. Moreover, the Blue Team can provide participants with offensive capabilities either to collect intelligence or destroy the enemy. The blue team works under participants' command and accepts the following commands:

1- Deceive and Watch: Channelling attacker into the deception service and collecting intelligence.
2- Reconnaissance: Scanning attacker and trying to find their weaknesses.
3- Destroy: Clearing the order to eliminate the enemy.
4- Active Intel: Either through channelling the attacker into deception or by utilising offensive action against enemy network to gather intelligence.

As explained in the induction session, participants will be asked to fill out answers to several questions during the experiment, and they may ask at any point to freeze the exercise.

c. ADX System And Network Typology:

1- HTTP server port 80
2- Database Server port 1433
3- VPN Server port 1723
4- Remote Share port 3389
5- Legacy system share port 445



3- LAB SURVEY:

PARTICIPANT INFORMATION SHEET

The purpose of this research is to explore the key factors associated with Cyber Situational Awareness and evaluate the strength of its association in order to validate comprehensive Active Cyber Situational Awareness model.

ELIGIBILITY REQUIREMENTS:
To be eligible to take part in this study you must be part of the following:
1- IT Security
2- Network Security
3- Cyber Incident Response Team
4- Cyber Defence

TIME COMMITMENT:
This Experiment should only take about 25 minutes of your time. Your answers will be completely anonymous unless you decide to provide your personal details

PROCEDURE & PARTICIPANTS' RIGHTS:
The research will be conducted through a lab experiment semi-structured survey where participation in this study is totally voluntary. Participants have the right to not take part of this experiment or withdraw at any time prior to submitting the questionnaire. The survey result will be collected anonymously unless participants decide to provide their personal detail. All data collected will be kept confidential and used for the purposes of this research only. All your personal data will be kept secure and protected under the Data Protection Act 1998, no other entity will be granted to access this research data. Any publication that may be derived from this survey will not include any sort of personal data.

BENEFITS AND RISKS:
There are no known benefits or risks for participants in this study

FOR FURTHER INFORMATION:
If you have any questions at any time about the study, please do not hesitate to contact Ahmed Al-Shamisi (ahmed.al-shamisi@brunel.ac.uk)

Demographic Information

1. Please fill the below questions:

Name:

Company:

Country:

Email Address:

2. What is your gender?

- ◯ Female
- ◯ Male

3. What is your age?

- ◯ 18 to 24
- ◯ 25 to 34
- ◯ 35 to 44
- ◯ 45 to 54
- ◯ 55 to 64
- ◯ 65 to 74
- ◯ 75 or older

4. What is the highest level of education you have completed?

- ◯ High school
- ◯ college
- ◯ Associate or bachelor
- ◯ Graduate degree
- ◯ Postgraduate

Name of your Degree

5. What is your job role?

- ◯ Networking
- ◯ IT Security
- ◯ IT Manager
- ◯ IT Forensic
- ◯ Programmer / Software Engineer
- ◯ Database Administrator
- ◯ System Administrator / Analyst
- ◯ Other

6. How large a role do you play in the IT Security of your Organization ?

- ◯ Extremely large
- ◯ Very large
- ◯ Moderately large
- ◯ Slightly large
- ◯ Not at all large

7. About how long have you been in your current position?

Years

8. Have done any of the following courses? Please select

- ☐ Computer Forensic
- ☐ IT Security
- ☐ Network Forensic
- ☐ IT Incident Response
- ☐ Ethical Hacking
- ☐ Network Security
- ☐ Other Hacking training
- ☐ Firewall and IDS

Participant SA

9. What is going on in the network ? What do you see ?

10. What does it mean?

11. What is your Situational Awareness?

12. What is your action toward the current situation?

4- PARTICIPANTS ASSESSMENTS SURVEY

Participant SA Evaluation

25. The correctness of the perception

- ◯ 1- Failed to Detect suspicious activities
- ◯ 2- Sensing there is something happening in the network but participant not sure yet
- ◯ 3- successfully identifies there is something wrong happing in the network
- ◯ 4- Successfully identifies there is suspicious activities in the network without identifying its type.
- ◯ 5- Successfully identify Enemy activity and the origin source of Attack

26. The Completeness of the perception

- ◯ 1- Participant Failed to Detect suspicious activities
- ◯ 2- Participant found there is something happening in the network but not sure yet
- ◯ 3- Participant managed to identifies there is something not normal in the network
- ◯ 4- Participant identifed there is suspicious activities in the network without identifying its type
- ◯ 5- Participant managed to get clear picture of the suspicious activities.

27. Participant Analysis capability

- ◯ 1- Failed to understand whats going on in the network
- ◯ 2- wrong judgment toward understanding the situation
- ◯ 3- part of the truth has been identifies where participants failed to provide clear picture of the situation.
- ◯ 4- successfully understood the the situation.
- ◯ 5- clear understanding of the situation and willingness to take action

28. Participant comprehension

- ◯ 1- Participants Failed to come up with a correct conclusion toward the situation
- ◯ 2- hesitation to take take action
- ◯ 3- several hypothesis has been made
- ◯ 4- high self confidence toward participant finding
- ◯ 5- trust in participant finding and willingness to take action

29. The Accuracy of captured information

- ◯ 1- Failed to capture the truth
- ◯ 2- part of truth has been captured but with wrong judgment
- ◯ 3- part of truth has been captured with successful judgment
- ◯ 4- accurate information has been captured but not sufficient enough to control incident
- ◯ 5- participant managed to captured accurate information that allowed him/her to predict future

30. The Timeliness of captured information

- ◯ 1- Failed to provide the information
- ◯ 2- information has been provided after the cyber incident
- ◯ 3- information has been provided during cyber incidents but late to control incident(Payload already executed)
- ◯ 4- information has been provided during cyber incidents where incident can be controlled
- ◯ 5- information has been provided before cyber incidents

31. Timeliness of Awareness building

- ◯ 1- Failed to provide SA
- ◯ 2- Partial of SA has been achieved after cyber incident
- ◯ 3- Partial SA has been achieved during cyber incident
- ◯ 4- SA has been achieved during cyber incident
- ◯ 5- SA has been achieved prior to cyber incident

32. The capability to act within a window of opportunity during the cyber incident

- ◯ 1- Failed to response to Cyber incident
- ◯ 2- Response and action was not appropriate to cyber incident
- ◯ 3- response to cyber incident was late
- ◯ 4- proper response was in place during cyber incident
- ◯ 5- proper response was in place prior to cyber incident

33. The capability to adapt to changes quickly

- ◯ 1- failed to adapt new measures
- ◯ 2- not sufficient measure has been adopted
- ◯ 3- new measure adapted late
- ◯ 4- adaptability to new measure was in place during cyber incident
- ◯ 5- adaptability to new measure was in place prior to cyber incident

34. Security Controls Utilisation.

- ◯ 1- Failed to utilise Security Dashboards
- ◯ 2- Used Dashboards to find there is suspicious activities after cyber incidents
- ◯ 3- Used Dashboards to find there is suspicious activities during cyber incident
- ◯ 4- Used Dashboards to find the source of suspicious activities before execution of cyber attack
- ◯ 5- utilisation of security controls to control cyber incidents(Block or Deceive)

35. Deception Utilisation

- ◯ 1- No Deception has been used
- ◯ 2- Deception used not correctly
- ◯ 3- Deception used after cyber incident
- ◯ 4- deception used during cyber incident
- ◯ 5- Deception used prior to cyber attack

36. Utilisation of Blue Team.

- ◯ 1- Failed to utilise Blue team
- ◯ 2- Poor and unclear command were given to blue team
- ◯ 3- Normal Passive order were given to blue team
- ◯ 4- Active and offensive order were given to blue team after cyber incident
- ◯ 5- Active and offensive order were given to blue team During cyber incident

37. Intelligence Reporting System.

- ◯ 1- Didn't rely on it
- ◯ 2- Use it incorrectly
- ◯ 3- Check it validity through exploring dashboards
- ◯ 4- Confident in take action
- ◯ 5- Use it without hesitation

38. The information used and participant knowledge and skill were reliable enough to build quality SA

- ◯ Yes
- ◯ No

Explain

39. Overall Participant SA and action in deterring cyber Incident

- ◯ Yes
- ◯ NO

Explain