This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/IWSSIP.2016.7502753, 2016 International Conference on Systems, Signals and Image Processing (IWSSIP). 23-25 May 2016 Bratislava Slovakia

Towards a Theoretical Framework for an Active Cyber Situational Awareness Model

Ahmed Al-Shamisi, Panos Louvieris, Mohammed Al-Mualla [1], Martin Mihajlov [2]

[1] Defence & Cyber Security Research Group, School of Information Systems, Computing and Mathematics, Brunel University Uxbridge, Middlesex, United Kingdom

{A.Al-Shamisi; Panos.Louvieris; Mohammed.Al-mualla}@brunel.ac.uk

[2] E-Business Department, Ss. Cyril and Methodius University, Skopje, Macedonia

martin@eccf.ukim.edu.mk

***Abstract*-While the mechanism and scope of cyberspace is progressing on a daily basis, risk factors and the ability to process cyberspace data in less time and using less effort are proving to be major roadblocks to achieve the desired outcomes. The defensive methods currently applied to counter these evolving attacks are not sufficient due to their preventive and reactive nature so an active posture is required. The passive natures of existing Situational Awareness (SA) models imply that they cannot enhance cyber SA in a world where there are new developments every day. The research activity in this paper focused on defining a new approach towards ensuring cyber security. We propose an Active Situational Awareness Model (ASAM) as a theoretical model that enhances the quality of cyber situational awareness. The model proposes a concept that conforms to the military stratagems of Sun Tzu, where operators always engage attackers directly by deploying active intelligence-gathering techniques in order to create new knowledge.**

***Keywords* — situational awareness, cyber situational awareness, active situational awareness model**

I. Introduction

The growth in technology has come with its fair share of challenges. One of the major challenges are cyber security threats, which have become a reality where criminal and terrorist activities are orchestrated across the globe [1]. Cyber threats, including, but are not limited to, fraud, identity theft, stealing corporate business secrets and cyber bullying [2]. Conversely, it can be concluded that in terms of technology cyber security is one of the major concerns in the modern world which calls for implementing measures to ensure safety.

Considering that the best defense is a strong offense, many countries have adopted this offensive strategy in order to deny criminal or terrorist forces in their attempts to control or use the Internet for their own illegal purposes through the creation of good botnets [3]. An active defense involves constant patrolling in cyberspace, in order detect, deny, pursue and deactivate websites, malicious software and other cyber agents owned by those with criminal and/or terrorist intentions [4]. In addition, patrolling provides more accurate information about future threats, including their source, resources and architecture. This information can enable an organization to upgrade its intelligence system to a higher level. In turn, this makes the organization far more capable of detecting attacks within the network including security credentials that have been compromised or data that has been stolen or destroyed [5].

This paper explores the state-of-the-art of Cyber Situational Awareness by investigating the existing situational awareness models and identifies their limitations when applied in the cyber domain. The main goal of this paper is to introduce a new theoretical framework that shapes an Active cyber SA model aimed to enhance cyber SA. In the next section we will investigate the existing Situational Awareness models and identify their limitations when applied in the cyber domain. Following, we will define a new active Situational Awareness model, in contrast to the existing passive models, which is in line with the military philosophy and strategies of Sun Tzu. Finally, we will discuss the potential drawbacks and the areas of research available when this model is applied in real-case scenarios.

II. Literature Review

Situational Awareness refers to the acquiring of knowledge about the environment and events occurring around us [6]. As a concept, SA has been extensively used in military combat operations for a long time [7]. As an area of research, its origins can be traced back to the theory of military grouping with the NCW [8], when research in military aviation security helped design computer boundaries for individual operators [9].

In the ICT industry, Situational Awareness is a more complex concept. It is defined as the capacity to swiftly and efficiently address arriving stimuli with appropriate responses [1O]. Considering the ICT dimension it is also referred to as Cyber Situation Awareness and it has become an ever-evolving field of interest. Denning's [11] pioneering work on using expert systems to detect computer attacks is marked as the beginning of Cyber SA. This seminal work was followed by a plethora of experiments covering areas such as anomaly detection, pattern matching, and agent-based systems [12]. The early stages of these experiments shaped the concept of data fusion, which was proposed in the JDL model [13]. As one of the first and most influential model in data fusion [14], the JDL model focuses solely on data management for preventing cyber-attacks.

The JDL model incorporates five levels for fusion methodologies including level O for preprocessing, level 1 for object refinement, level 2 for situation refinement, level 3 for threat refinement, and level 4 for process refinement. The stream of data enters the model at level O, which provides physical access to the raw bits or signal. Based on signal level data association and characterization, the model estimates the existence of an object. The objects are correlated and tagged in order to perform object identification during level 1 processing.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/IWSSIP.2016.7502753, 2016 International Conference on Systems, Signals and Image Processing (IWSSIP). 23-25 May 2016 Bratislava Slovakia

In an attempt to understand the current situation, the knowledge of objects, their characteristics and relationships with each other are aggregated during level 2 processing. Following, the assessment of the impact of the given situation proceed at level 3. The impact estimate includes likelihood estimates and cost/utility measures associated with the potential outcomes of a player's planned actions. Finally, the last level provides a feedback mechanism to the other layers, including the sensor itself. In the revised JDL model [15], level 4 process refinement might include both the user and sensor control functions as feedback for refining the fusion process.

The main significance of the JDL model for SA lies in the fact that the model highlighted the importance of algorithmic techniques in support of situation awareness [16]. Nevertheless, even though the JDL model was developed to define the fusion process it is useful only for automatic processing of a machine and does not account for human processing. As a solution, Blasch & Plano [17] proposed an additional level to this model, level 5 for user refinement in order to delineate the human from the machine in process refinement. Dasarathy [18] introduced the fusion-focused Data-Feature-Decision (DFD) model to guide a machine to make decisions based on data. In the Omnibus model [19], which acts as an extension of the OODA control loop, the machine is central to the model and is based on a human reasoning strategy.

Cyber situational awareness refers to knowledge about ongoing events in the cyber environment making human elements significantly important in the process of achieving quality. As the JDL model does not model the data fusion process from a human perspective, Endsley [2O] proposed a model that consolidated the theoretical perspective of SA by adding human factors. This model consists of two main parts, where the first part is considered as the core of SA, while the second part deals with the various factors affecting SA.

The core portion introduces the three levels of mental representation in SA: perception, comprehension, and projection. On level 1, perception provides information about the status, attributes and dynamics of the relevant elements in the environment. The perception of important information appears fundamental in the correct visualization of the occurring situation [21] and provides the basic building blocks for the following levels. This claim is supported by the finding that 76% of SA errors made by the pilots stemmed from lack of perception of the required information [22]. On level 2, comprehension refers to an outcome relating to how people interpret, associate, store and retain information. This includes the integration of multiple pieces of information and a determination of their relevance to the underlying goals in order to produce a composite picture of the evolving situation. In the previously mentioned study, lack of comprehension was a cause of 2O% of pilot error. Projection, placed on level 3, helps decision-makers with the highest level of SA, to forecast the occurrence of situational events and their progression dynamics. The second part of Endsley's model presents an elaborate and detailed description of the various factors affecting SA such as elements, time and space. Nevertheless, a successful fusion system must address the entire process which includes data acquisition, awareness, prediction and the ability to request elaboration or additional data. For this reason, the Endsley's model has been extended to a fourth level, Resolution, which provides awareness of the best path to follow to achieve the desired outcome to the situation [23].

Endsley's model is a purely cognitive theory which not only depends on information flow, but also does not consider technological factors. As such, the model is too abstract and doesn't state how SA is achieved in detail, making it insufficient for cyber security. In the perceptual cycle model [24] and the activity theory model [25], the psychological approach to SA is different, nevertheless all of the models are still defined as constricting parallel processes. Tadda [26] identifies the JDL model as a bottom-up, data-driven functional model, and the Endsley's model as a top-down, goal-driven mental model. He correctly recognized the value of both approaches, and proposed a combined model. In his SA model the levels of the JDL model are initially split into two different processes. Levels O (data acquisition) and level 1 (object correlation), are treated as a single process by defining the objects structures within the object's identification modules. Levels 2 and 3, have been placed into another process devoted solely to situation assessment.

Functionally, this model contains the best elements of both JDL and Endsley's models, with some additional items such as initial data requirement and textual input. This combined SA model defines the problem/goal in a top-down manner through a so-called processing flow solution, where actions such as projection (alerts), comprehension (model analysis), perception (data collection), parsing/extraction and data cleansing take place. Following, process refinement deals with missing data, additional data and input for sensor management until the model reaches the process of offline-processing which involves knowledge discovery. The model uses three broad areas of operation: perception, comprehension, and anticipation, which can be applied to cyber SA. Evidence is collected at the perception level, on the comprehension level the situation is understood by recognizing intrusion attempts and exploiting a priori knowledge, which in turn would enable the anticipation of the possible magnitude of impact [27].

Tadda himself identifies the main weakness in his model in the difficulty to determine possible futures. At level 2 the prevention of an actual attack falls short simply because the knowledge of the defender is less than the knowledge of the attacker. This diminished knowledge occurs because in Tadda's model data is only captured from local networks and not cyberspace. Cyber Situational Awareness must consider the other effects of a cyber-attack, beyond network data. Local network monitoring can never detect zero day attacks, therefore it is necessary to obtain intelligence on the enemy network as well.

III. Active Situational Awareness Model

All of the current SA models show a preference for a defensive posture when it comes to deterring cyber-attacks. They influence the operator to process and utilize knowledge only within the concept of attack prevention which creates a defensive mindset. An attitude of only blocking the attackers is never sufficient to win the situation; instead, it motivates enemies to become more innovative and produce new and creative ways of attack. Conversely, the models suffer from

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/IWSSIP.2016.7502753, 2016 International Conference on Systems, Signals and Image Processing (IWSSIP). 23-25 May 2016 Bratislava Slovakia

uncertainty because their focus on self-awareness confines their activities within the host domain as new knowledge is always required in order to prevent an attack [28]. The following section of this paper presents a modeling strategy with a proactive approach towards Situational Awareness. This model is strongly influenced by Sun Tzu's military strategy and the dynamics of an offensive posture to deter cyber-attacks.

A. Theoretical Framework

A classic passive cyber network defense 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 [29]. The passive pre-defined techniques that, for example, disable an account or notify an administrator, are inadequate in the sense that hackers devise techniques to circumvent these measures and launch successful attacks [3O]. In contrast, an active defense comprises measures originated by the defender against the attacker, which will not only prevent attacks in progress, but would ideally make it difficult for the attacker to launch more attacks. Active SA and active defense techniques can be divided into three categories:

- **Counterattack -** conducted against the attacker's information system during or immediately after the initial attack.
- **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.
- **Active deception -** uses the momentum of the attack to defeat it by channeling an attack away from the defender's information scheme and into a parallel dummy system.

With this in mind and considering the previously reviewed literature, a theoretical framework for active Situational Awareness should consider the following points.

1. The cyber commander should possess an offensive attitude/mindset towards all cyber-attacks.
2. The offensive attitude should encourage the operator to decisively create new knowledge.
3. The cyber commander should create and exploit the acquired new knowledge through an appropriate active SA model to enable the operator to exploit multi-domain ambience, invade attackers' domains, and apply deception tactics.
4. The aggressive strategy should defeat the attackers before they can resort to any harmful operation within the operator's domain.
5. The operator should be able to achieve the desired outcome, i.e., manage, retain and improve the desired cyber operations.

B. Compact Theoretical Model

Organizations 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. Therefore, within the previously discussed theoretical framework, an active SA model needs to complement the winning attitude and enable the cyber commander to employ an appropriate defensive technique in a multi-domain environment.

Within this context, the tasks of the Active SA Model (ASAM) proposed in this study can be framed as follows:

- ASAM will interact with adversaries;
- ASAM will be activated once an attack gets redirected;
- ASAM will use deception by redirecting the attacker to a deception server;
- ASAM will use spyware, to control the adversaries and to get into their domain;
- ASAM will influence the enemy through deception, which will affect their own SA.

These tasks highlight the role of intelligence as creation and application of new knowledge. The new knowledge generated by ASAM would act as a force multiplier helping us to narrow down the role of ASAM in a compact theoretical model.

C. Alignment with Sun Tzu's Strategies

The role of intelligence is extremely crucial in the ASAM model since new knowledge will form the basis of a counter action. In addition, the model needs to be continually updated with knowledge about the capabilities, resources, plans and motives of the potential attackers. The existing literature offers no solution within this context, except for the concept put forward by Sun Tzu [31], which specifically focuses on how the intelligence of one party can be used to defeat the other. His strategy is applicable in cyber situation since it covers all possible situations, especially when the issue of intelligence is involved. The integration of networks takes place in the mind of the commander, but by deception in cyberspace, the mind of the commander can be attacked [32]. Hence, in a cyber war, commanders should direct their intelligence operations towards gathering information that will deny cyber attackers from achieving their purpose. Considering the gravity of the threat to cyber security, the proposed ASAM will integrate military philosophy in its structure and mechanism by utilizing 13 military recommendations from Sun Tzu's Art of War (AoW) under four categories. These categories, initiation, direction, action, and exploitation, will shape the process of active defense.

1) Initiation

During Initiation ASAM allows the commander to deal with basic knowledge in order to formulate the basic course of action by utilizing 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 [31], [33]. 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 defense goal should be to improve an organization's ability to collect, evaluate and transmit digital evidence [34].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/IWSSIP.2016.7502753, 2016 International Conference on Systems, Signals and Image Processing (IWSSIP). 23-25 May 2016 Bratislava Slovakia

Considering that both AoW's accent the importance of gathering appropriate inputs about the enemy, the four variables important for this category are: enemy identity, enemy location, enemy motive and enemy goal. These will establish the fundamental knowledge which the commander cannot do without. Accordingly, the activities that fall under this category 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.

2) Direction

Besides understanding the magnitude of the enemy's strength, in this phase, ASAM would develop a detailed plan. The model will utilize AoW IX (Army on the March) and AoW X (Terrain). In accordance with AoW IX, cyber commanders need to check all nuances of the system while counter attacking the enemy, while simultaneously remembering that attackers can also apply deception [31]. AoW X suggests that cyberspace contains more dangers than the real world, since terrestrial distance does not play a role in a network. Hence, it will be necessary to apply meticulous pre-operational cyber-attack planning in order to manage the cyber terrain [33].

These AoWs stress the importance of gauging the enemy from all sides, creating three variables of importance, Enemy Capability, Enemy Weakness and Possible Impact of Enemy Attack. Accordingly, the activities within this category would involve the use of the Explicit Knowledge acquired from activities during Initiation.

3) Action

Action is the most elaborate phase of the model as commanders launch an attack on a cyber explorer who has already been tracked down as a potential threat. At this stage the ASAM would allow commanders to utilize 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).

AoW II. To ensure the safety of the domain, the cyber commander would collect the credentials and privileges of the enemy without disclosing this action to the enemy [35], [36].

AoW III. When the cyber-attack involves the IT infrastructure the commander needs to secure victory before combat is even necessary [31].

AoW V. In a win-or-perish situation the enemy might focus all available power and skill to outmaneuver the commander. Therefore, the commander must remain one step ahead and attack the opponent at the most opportune moment [34].

AoW VI. The commander will make all cyber reconnaissance tasks difficult and confusing to the enemy, in order to prevent the enemy from developing an effective strategy [31].

AoW VII. The commander will deceive the enemy through misinformation before going for the final decisive attack [33].

AoW VIII. The commander will treat every combat as a new situation and approach it with alacrity, disregarding the potential complacency from earlier success [31].

AoW XI. The commander will monitor all nuances of the system while counter-attacking the enemy [31].

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.

4) Exploitation

In Exploitation, ASAM would work on exploiting the enemy in order to extract more knowledge about the motives and goals behind the attack. Here, ASAM would utilize AoW XII (Attack by Fire) and AoW XIII (Use of Spies). AoW XII suggests that the commander should annihilate the enemy, while AoW XIII suggests using spies to get more information in such a situation.

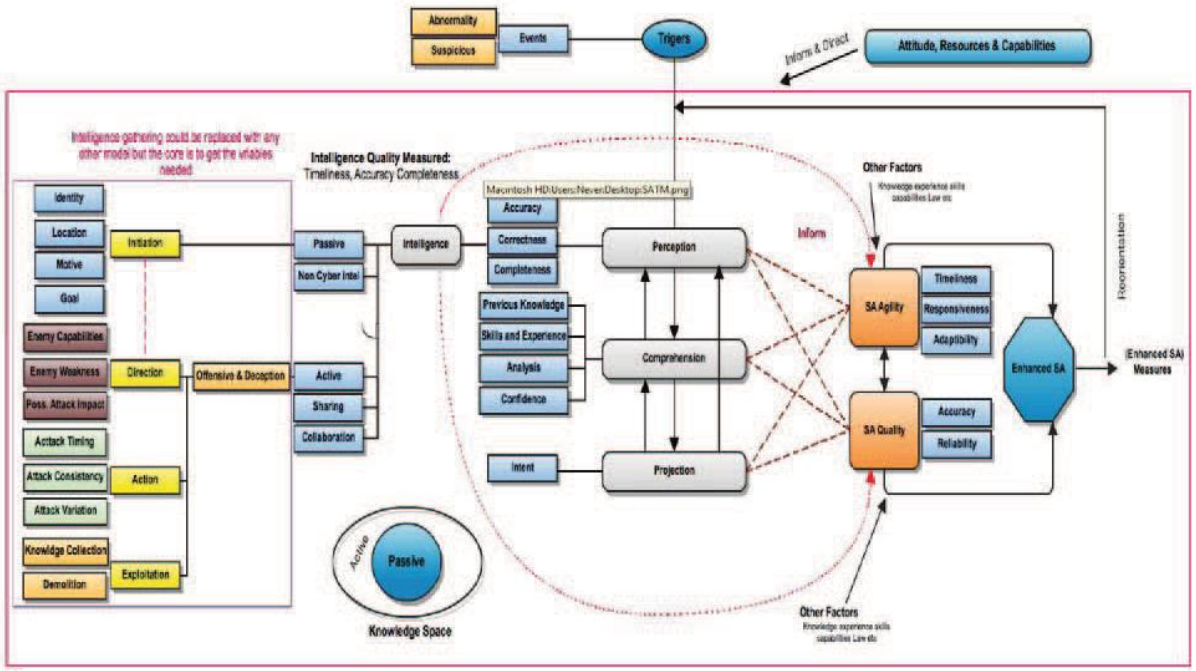

Fig. 1. Detailed Theoretical Active Situational Awareness Model

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/IWSSIP.2016.7502753, 2016 International Conference on Systems, Signals and Image Processing (IWSSIP). 23-25 May 2016 Bratislava Slovakia

This would lead the commander to deal with two variables: Knowledge Collection and Demolition. Knowledge Collection and Demolition can work in tandem in order to enable the commander to launch both offensive and deception activities.

D. Detailed Theoretical Active Situational Awareness Model

Considering all of the aspects discussed so far the enhanced theoretical model of ASAM is presented in Figure 1.

In this model, the three major components inherited from the passive SA models, perception, comprehension and projection, would depend on the qualities of several factors. 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.

In order to effectively enhance situational awareness, ASAM has to be implemented via a specific process carried out in three major steps. The first step is the alert stage which is noted through passive action [37]. This aims at procuring relevant information such as the attacker's identity, motive, location, goal, capability, weakness and impact. The second step is high level interaction, where the enemy domain is actively attacked. Potential information that can be discovered includes the attacker's operating system, opened ports and active services [38]. This identifies the weaknesses of the attacker's domain and provides the necessary information for countering the attack [39]. In the last step of the process, resource database mobilization, the active domain is prepared to counter the attack. The identified vulnerabilities are patched and the necessary protective measures which would ensure that the domain remains safe and impenetrable to the attackers are activated.

IV. Discussion

The threats of cyber-attacks are always evolving. Cyber incidents can happen in a fraction of second, and therefore it is necessary to have an agile response to deter attacks and defend computer networks. This paper has identified and explained the variables of the new, enhanced SA model, where intelligence factors directly impact SA. The enhanced Situational Awareness in this model is achieved by utilizing an offensive capability which allows defenders to interact with suspected attackers in order to gain new knowledge. This approach makes active intelligence a critical component of the enhanced SA model, as it has been argued that passiveness in cyber security is inadequate [26]. The cumulative power of active intelligence in ASAM would greatly enhance SA, which in turn would help the commander to confront and defeat the potential enemy.

Arguably, one of the main questions that might arise for the proposed model is how ASAM could perform so many tasks. As discussed previously the main driving force of ASAM is intelligence generated from new knowledge gathered from the adversary domain. With this knowledge the commander can operate with enhanced ability to deter cyber-attacks since it is consistent with military doctrine. A continuous flow of intelligence would give the upper hand to the operator dealing with security threats even before their occurrence. For example, ASAM could influence the attacker by exploiting the OODA loop [4O], where the central tenet, stemming from a military perspective, is to defeat the adversary strategically, by psychological paralysis [2].

On its own, Situational Awareness is a combination of perception, comprehension and projection. Researchers have discussed how information feeds into perception; however, they have not been clear about what to perceive (Endsley, 1995; Tadda, 2OO8). Tadda's model provides some basic information about data-gathering and the importance of intelligence feeding at level O of his model, but does not explicitly cover what information is to be gathered. The current passive SA models relay only the information that comes from the local domain, while on the other end of the spectrum, the core of the proposed ASAM in this paper is the active intelligence factor. In ASAM, this active intelligence comes from previous knowledge or experience regarding cyber incidents, risk assessments of cyber resources, politics or deception, whereas adversaries can be channeled into manageable or controlled cyber resources for the purpose of gathering intelligence. Conversely, 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.

V. Conclusion

The theoretical findings in this research identify the set of actions proposed by ASAM as most adequate for cyber security due to its active, offensive nature. Unlike other models, ASAM helps in gathering highly accurate intelligence attained offensively by hacking the enemy's domain. As such the gather intelligence has all the desired characteristics of cyber intelligence: accuracy, completeness, timeliness and reliability. Consequently, the decisions made with regard to the data are well informed, and the protective measures derived from this information are precise and customized to counter specific enemy attacks.

Nevertheless, ASAM still requires the rigors of evaluation through real-time laboratory testing on a cyber range to prove its efficacy and effectiveness. Current SA models have no mechanisms that allow us to assess the advantages of a particular model. Therefore, it is very important to have a measurement factor that determines how good is the personnel SA by measuring the quality of their SA and their agility in achieving it. Enhanced SA can be measured by using quality and agility variables to determine how good the SA performance is, which is critical to SA evaluation. In future research we plan to identify the variables necessary to develop a framework for assessing SA. We would then use these variables to test the utility of the proposed ASAM in practice using the cyber range in a Serious Gaming Experiment. This approach to SA evaluation will not only serve to evaluate whether ASAM enhances SA, but also provide the means to directly measure SA performance in order to determine SA Training.

References

[1] H. Lin, "A virtual necessity: Some modest steps toward greater cybersecurity," *Bull. At. Sci.*, vol. 68, no. 5, pp. 75-87, 2O12.

[2] A. Ben Aissa, R. K. Abercrombie, F. T. Sheldon, and A. Mili, "Defining and computing a value based cyber-security measure," *Inf. Syst. E-bus. Manag.*, vol. 1O, no. 4, pp. 433-453, 2O12.

[3] C. A. Theohary and J. Rollins, "Terrorist Use of the Internet: Information Operations in Cyberspace," 2O11.

[4] E. Varon, "SECURITY LEGISLATION - Homeland Defense: New Rules of War after 9/11," *CIO*, 2OO2. [Online]. Available: http://www.cio.com/article/3O8O5/SECURITY LEGISLATION Homeland Defense New Rules of War after 9 11.

[5] HBGary, "Active Defense," *HBGary*, 2O13. [Online]. Available: http://hbgary.com/products/active defense.

[6] M. J. Adams, Y. J. Tenney, and R. W. Pew, "Situation Awareness and the Cognitive Management of Complex Systems," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, no. 1. pp. 85-1O4, 1995.

[7] J. Harrald and T. Jefferson, "Shared situational awareness in emergency management mitigation and response," in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*, 2OO7, pp. 23-23.

[8] D. S. Alberts, *Network Centric Warfare*. 2OOO.

[9] M. R. Endsley, "Automation and situation awareness," in *Automation and Human Performance: Theory and Applications*, 1996, pp. 163-181.

[1O] L. D. Cumiford, "Situation Awareness for Cyber Defense: Knowledge Discovery and Extraction Defense Systems and Assessments." Sandia National Laboratories, 2OO6.

[11] D. E. Denning, "An Intrusion-Detection Model," *IEEE Trans. Softw. Eng.*, vol. SE-13, no. 2, 1987.

[12] D. E. Denning, "Activism , Hacktivism , and Cyberterrorism : the Internet As a Tool for Influencing Foreign Policy," *Networks Netwars Futur. Terror. Crime, Militancy*, pp. 239-288, 2OO1.

[13] D. L. D. L. Hall, S. Member, and J. Llinas, "An introduction to multisensor data fusion," *Proc. IEEE*, vol. 85, no. 1, pp. 6-23, 1997.

[14] R. K. Srihari, W. Li, T. Cornell, and C. Niu, "InfoXtract: A customizable intermediate level information extraction engine," *Nat. Lang. Eng.*, vol. 14, no. June, pp. 51-58, 2OO8.

[15] A. N. Steinberg, C. L. Bowman, and F. E. White, "Revisions to the JDL data fusion model," *Proc. SPIE*, vol. 3719, no. 1, pp. 43O-441, 1999.

[16] J. Salerno, "Measuring situation assessment performance through the activities of interest score," in *Proceedings of the 11th International Conference on Information Fusion, FUSION 2008*, 2OO8.

[17] E. P. Blasch and S. Plano, "JDL level 5 fusion model: user refinement issues and applications in group tracking," in *Proceedings of SPIE*, 2OO2, vol. 4729, pp. 27O-279.

[18] B. V. Dasarathy, "Sensor fusion potential exploitation-innovative architectures and illustrative applications," *Proc. IEEE*, vol. 85, no. 1, pp. 24-38, 1997.

[19] M. Bedworth and J. O'Brien, "The Omnibus model: a new model of data fusion?," *Ieee Aerospace And Electronic Systems Magazine*, vol. 15, no. 4. pp. 3O-36, 2OOO.

[2O] M. R. Endsley, "Measurement of Situation Awareness in Dynamic Systems," *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol. 37, no. 1. pp. 65-84, 1995.

[21] M. Endsley, R. Sollenberger, and E. Stein, "Situation Awareness: A Comparison of Measures," *Proc. Hum. Performance, Situat. Aware. Autom. User Centered Des. New Millenn. Conf.*, 2OOO.

[22] M. R. Endsley and C. A. Bolstad, "Individual Differences in Pilot Situation Awareness," *The International Journal of Aviation Psychology*, vol. 4, no. 3. pp. 241-264, 1994.

[23] B. McGuinness and L. Foy, "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*, 2OOO.

[24] K. Smith and P. a. Hancock, "Situation Awareness Is Adaptive, Externally Directed Consciousness," *Hum. Factors J. Hum. Factors Ergon. Soc.*, vol. 37, no. 1, pp. 137-148, 1995.

[25] G. Bedny and D. Meister, "Theory of Activity and Situation Awareness," *Int. J. Cogn. Ergon.*, vol. 3, no. 1, pp. 63-72, 1999.

[26] G. P. Tadda, "Measuring performance of cyber situation awareness systems," in *Proceedings of the 11th International Conference on Information Fusion, FUSION 2008*, 2OO8.

[27] P. Barford, M. Dacier, T. G. Dietterich, M. Fredrikson, J. Giffin, S. Jajodia, S. Jha, J. Li, P. Liu, P. Ning, X. Ou, D. Song, L. Strater, V. Swarup, G. Tadda, C. Wang, and J. Yen, "Cyber SA: Situational awareness for cyber defense," *Adv. Inf. Secur.*, vol. 46, pp. 3-13, 2O1O.

[28] G. P. Tadda and J. S. Salerno, "Cyber Situational Awareness," *Inf. Secur.*, vol. 46, no. 3, pp. 139-154, 2O1O.

[29] J. M. Beaver, C. A. Steed, R. M. Patton, X. Cui, and M. Schultz, "Visualization techniques for computer network defense," 2O11, vol. 8O19, pp. 8O19O6-8O19O9.

[3O] E. J. Holdaway, "Active Computer Network Defense: An Assessment," DTIC Document, 2OO1.

[31] R. D. Sawyer, *Sun-tzu: The art of war*. Basic Books, 1994.

[32] E. Nakashima, "Defense official discloses cyberattack," *Washington Post*, vol. 24, 2O1O.

[33] R. C. Park and D. P. Duggan, "Principles of Cyber-warfare." IEEE, 2OO1.

[34] K. Geers, *Strategic Cyber Security*. 2O11.

[35] R. Addinall, "Information in Warfare from Sun Tzu to the 'War on Terror,'" in *Security and Defence: National and International Issues, 7th Annual Graduate Student Symposium*, 2O12, pp. 457-477.

[36] K. Geers, "Sun Tzu and Cyber War," *CCD CoE*, pp. 1-23, 2O11.

[37] G. B. Palermo and R. N. Kocsis, *Offender Profiling: An Introduction to the Sociopsychological Analysis of Violent Crime*. Charles C Thomas Publisher, 2OO5.

[38] W. Wang, *Steal this computer book 4.0: what they won't tell you about the Internet*. No Starch Press, 2OO6.

[39] S. Gordon, "Geographic flexibility will boost prospects," *Comput. Wkly.*, p. 54, 2OO5.

[4O] J. R. Boyd, "Organic design for command and control," *A Discourse Win. Losing*, 1987.