NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A CYBER SITUATIONAL AWARENESS MODEL FOR NETWORK ADMINISTRATORS

by

Huseyin Karaarslan

March 2017

Thesis Advisor: Alan Shaffer
Co-Advisor: John Gibson

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2017	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE A CYBER SITUATIONAL AWARENESS MODEL FOR NETWORK ADMINISTRATORS		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Huseyin Karaarslan			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U. S. Government. IRB number ____N/A____.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.		**12b. DISTRIBUTION CODE**	

13. ABSTRACT (maximum 200 words)

Although there are many well-established cyber security tools and techniques available to network administrators for managing and defining their systems, attackers still succeed in penetrating their systems. Defending these systems' confidentiality, integrity, and availability is the responsibility of network administrators; however, protecting these systems becomes more difficult when one considers the volume and velocity of data provided by many of these cyber security tools. Often this data may actually indicate a cyber-attack, but is hard to discern among the bulk of data provided. The purpose of this research is to propose a cyber situational awareness (CSA) model to provide network administrators with better situational awareness of cyber security threats to their systems. This research examines an established situational awareness model and surveys cyber security practices and tools to extend this knowledge to actual cyber situational awareness. This research further develops a model for CSA in three hierarchical levels: configurational awareness, operational awareness, and special conditions awareness. The research concludes that if network administrators manage their systems with awareness of these three levels, they would be able to decrease the amount of unnecessary data and focus on the most important information that can help them better guarantee cyber security of their systems.

14. SUBJECT TERMS network administrator training, network management, network configuration, cyber situational awareness, operational awareness, configurational awareness, cyber situational awareness pyramid, cyber-security tools, cyber-security techniques			**15. NUMBER OF PAGES** 63
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

A CYBER SITUATIONAL AWARENESS MODEL FOR NETWORK ADMINISTRATORS

Huseyin Karaarslan
Captain, Turkish Gendarmerie
B. S., Turkish Military Academy, 2007

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2017

Approved by: Alan Shaffer, Ph.D.
Thesis Advisor

John Gibson
Co-Advisor

Dan C. Boger, Ph.D.
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Although there are many well-established cyber security tools and techniques available to network administrators for managing and defining their systems, attackers still succeed in penetrating their systems. Defending these systems' confidentiality, integrity, and availability is the responsibility of network administrators; however, protecting these systems becomes more difficult when one considers the volume and velocity of data provided by many of these cyber security tools. Often this data may actually indicate a cyber-attack, but is hard to discern among the bulk of data provided. The purpose of this research is to propose a cyber situational awareness (CSA) model to provide network administrators with better situational awareness of cyber security threats to their systems. This research examines an established situational awareness model and surveys cyber security practices and tools to extend this knowledge to actual cyber situational awareness. This research further develops a model for CSA in three hierarchical levels: configurational awareness, operational awareness, and special conditions awareness. The research concludes that if network administrators manage their systems with awareness of these three levels, they would be able to decrease the amount of unnecessary data and focus on the most important information that can help them better guarantee cyber security of their systems.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. OVERVIEW....1
B. PROBLEM STATEMENT....3
C. PURPOSE STATEMENT....3
D. RESEARCH QUESTIONS....3
E. RESEARCH METHODS....4
F. POTENTIAL BENEFITS, LIMITATIONS, AND RECOMMENDATIONS....4

II. LITERATURE REVIEW....5
A. OVERVIEW....5
B. CYBER SITUATIONAL AWARENESS....6
1. Level 1 SA: Perception of the Elements in the Environment....8
2. Level 2 SA: Comprehension of the Current Situation....10
3. Level 3 SA: Projection of Future Status....11
C. MAVNATT....11
D. SUMMARY....13

III. SURVEY OF NETWORK AWARENESS TOOLS AND TECHNIQUES....15
A. NETWORK SECURITY AND AWARENESS TECHNIQUES....16
1. Access Control Lists....17
2. Security Technical Implementation Guides....18
3. System Logs....20
B. NETWORK AWARENESS TOOLS....21
1. Firewalls....21
2. Intrusion Detection Systems....22
3. Intrusion Prevention Systems....24
4. Anti-Virus Software....24
5. Nagios XI....25
6. NetCrunch....26
7. Solaris Network Performance Monitor....27
8. Host Based Security System....29
C. SUMMARY....29

IV. CYBER SITUATIONAL AWARENESS MODEL DESIGN....31

A. CYBER SITUATIONAL AWARENESS PYRAMID 32
1. Configurational Awareness 33
2. Operational Awareness 34
3. Special Conditions Awareness 35
B. SUMMARY 36

V. CONCLUSION AND FUTURE WORK 37
A. SUMMARY AND CONCLUSION 37
B. FUTURE WORK 38

LIST OF REFERENCES 41

INITIAL DISTRIBUTION LIST 45

LIST OF FIGURES

Figure 1. Model of Situational Awareness in Dynamic Decision Making. Source: Endsley (1995). 8

Figure 2. MAVNATT Conceptual Model. Source: McBride (2015). 12

Figure 3. DISA STIG Viewer 19

Figure 4. Nagios XI Infrastructure Management Feature, Example of Network Replay Report. Source: “Nagios XI” (2016). 26

Figure 5. NetCrunch Pending Alerts View, Example Display. Source: “NetCrunch” (n.d.). 27

Figure 6. Solaris NPM Network Availability and Performance Monitoring Screenshot. Source: “SolarWinds” (n.d.). 28

Figure 7. Cyber Situational Awareness (CSA) Pyramid. 33

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Vulnerability Severity Category Code Definitions. Source: “STIGs Home” (n.d.). 19

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACL	Access Control List
AV	anti-virus
CA	configurational awareness
CSA	cyber situational awareness
DDOS	distributed denial of service
DISA	Defense Information Agency
DOD	Department of Defense
DoS	denial of service
GUI	graphical user interface
HBSS	Host Based Security System
HIDS	host-based intrusion detection system
IDS	intrusion detection system
IoT	Internet of things
IPS	intrusion prevention system
IT	information technology
MAVNATT	Mapping, Awareness, and Virtualization Network Administrator Training Tool
NIDS	network-based intrusion detection system
NPM	Network Performance Monitor
NPS	Naval Postgraduate School
OA	operational awareness
SA	situational awareness
SCA	special conditions awareness
STIG	Security Technical Implementation Guide
XML	Extensible Markup Language

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my advisors, Alan Shaffer and John Gibson, for being such great advisors to me. You spent a lot of time with me, enabling me to succeed and finish my proposal and thesis on time. I will remember your contributions to my knowledge and expertise my whole my life. Thank you.

To my lovely wife, Sebahat. You have been enormously supportive to me since we got married. You are always with me for every moment of my life. While I have been studying at NPS, you dedicated yourself to me. I have completed this thesis with the motivation I got from you and our son, Ihsan. I will love you forever.

I also want to thank my great friends I met at NPS. You made me enjoy every moment at NPS.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. OVERVIEW

Vulnerabilities inside cyber systems are of primary interest to cyber attackers since every vulnerability opens a new door for a threat to exploit. This is especially true for large military or governmental organizations, where these vulnerabilities may result in serious risks to critical national security systems.

Cyber system vulnerabilities may be a result of untrained system users, insider threats, or weaknesses in the systems themselves. For example, a user who is not allowed to use a flash drive on an organizational computer, but nonetheless uses one without knowing what is stored on the flash drive may inadvertently cause malicious software to penetrate the network. Alternately, a malicious insider may do essentially the same thing, but intentionally and secretly, or may change system settings to create a security vulnerability or create even more damage not seen by system administrators. The systems themselves are not always designed to correspond to best-known security practices; for example, the default configuration that may be appropriate and sufficiently secure for one system may on another system disclose information without the knowledge of the system administrator. Additionally, installation of new software or hardware on the network could cause system vulnerabilities due to incompatibility with system security policies implemented by the system administrator.

When it comes to system security management, threats can be an issue. Although there are many tools for identifying threats and vulnerabilities, the data these tools provide is often not clear enough for human decision makers to use effectively. As these tools may produce large amounts of data, the network administrator must decide what data reflect a vulnerability. Furthermore, some vulnerabilities result from routine system data or installed software and patches. This task becomes particularly challenging when one considers that very critical systems, such as military or governmental systems, must be monitored actively to prevent threats from penetrating critical systems or to make the administrator aware of unintentional system state changes. For these reasons, maintaining active awareness of cyber system configurations and security posture is a critical role for cyber system administrators.

However, network administrators' situational awareness capabilities depend on their experience, training, and knowledge. Ideally, a real-time training environment can provide administrators with the necessary knowledge and experience without affecting the real system. For that purpose, Naval Postgraduate School (NPS) student Daniel McBride designed the Mapping, Awareness, and Virtualization Network Administrator Training Tool (MAVNATT) in his 2015 thesis. In this tool, McBride outlined three different modules integrated to create a virtual environment for training tactical network administrators and monitoring locally deployed systems. The main idea of the awareness module is to visualize the network topology and to integrate fault detection capabilities within MAVNATT. He stipulated that the awareness module must be able to develop network administrators' situational awareness. He identified existing tools to generate the awareness capability; however, these tools were not convenient solutions to implement in the virtual training environment (2015). Nonetheless, his thesis showed the importance of training to develop network administrators' situational awareness.

As previously stated, cyber systems security and maintenance largely depend on well-trained network administrators who know how to use their tools and understand what is happening in their network systems. That is why these administrators need to be trained in real-time virtual environments, such as that provided by MAVNATT. Hence, tools, training methods, and best practices should be identified and, where possible, incorporated in MAVNATT to provide an environment capable of enhancing network administrators' situational awareness.

In this context, situational awareness refers to the extent to which one is aware of the system's configuration, operation, and special conditions. Poor system configurations may expose vulnerabilities. For this reason, implementing known best practices for system configuration generally results in a more secure system. Yet, the best system configurations may not be enough to prevent vulnerabilities if an administrator is not actively aware of the system's operation. Administrators must monitor the devices in their systems to be sure they are all working as expected. Nonetheless, even though everything seems normal, sometimes special conditions may occur in the system state that may be difficult for the administrator to detect or interpret. Maybe an attack on the

system, either by external or insider operatives, is trying to change something to make the system vulnerable to more extensive exploits. Moreover, as the technology develops, many other vulnerabilities may become evident in the system. Therefore, the administrator's capability to understand, evaluate, and mitigate vulnerabilities is important and needs to be developed, assessed, and exercised.

B. PROBLEM STATEMENT

Although many tools exist to assess vulnerabilities and monitor cyber threat activities within tactical networks, network administrators lack the ability to continuously maintain cyber situational awareness over these networks, particularly in the context of fielded, operational, and time-critical systems.

C. PURPOSE STATEMENT

The purpose of this research is to understand cyber situational awareness (CSA) with regard to the perspective of network administrators and provide a model for enhancing the training methods and contexts for network administrators with respect to actively maintaining situational awareness over their systems, particularly against cyber threats and vulnerabilities. This research evaluates existing tools and best practices pertinent to establishing and maintaining an awareness of network status and operations and, based on that evaluation, recommends cyber security methods by which network administrators can increase their awareness of network status indicators.

D. RESEARCH QUESTIONS

This research's goal is to better understand cyber situational awareness. Therefore, these questions will be the main focus of this thesis.

1. What is cyber situational awareness?

    - What tools are being used for cyber situational awareness?
    - What are the best practices for secure systems?
    - How might cyber situational awareness by modeled so as to guide system administrator training and evaluation?

2. How can the effectiveness of the network administrator's situational awareness be increased?

   - What tools are needed to enhance the administrator's awareness?
   - What inhibits the network administrator's awareness?

E. RESEARCH METHODS

This research examines previously published literature, including cyber security and awareness reports, surveys, government and enterprise publications, and other research papers to discover appropriate best practices, training methods, and tools used for maintaining situational awareness of network administrators in the context of cyber systems. Best practices may include network training methods, configuration settings, or cyber security tools.

Initially, the research addresses the concept of situational awareness in large enterprise networks. The aim is to survey the types of threats and exploitations observed by administrators of such networks to better clarify what it means for an administrator to be "aware" of his network. To this end, we survey existing situational awareness tools and best practices in the cyber security domain to examine how they may support administrator awareness of the network.

Finally, the research identifies tools and techniques that can be used to develop the effectiveness of network administrators with respect to finding vulnerabilities and threats in tactical networks and make recommendations as to how such tools may be adopted or adapted for use by MAVNATT.

F. POTENTIAL BENEFITS, LIMITATIONS, AND RECOMMENDATIONS

This thesis is intended to help network administrators gain a better understanding of the means and methodology of establishing situational awareness for enhancing system security; it will lead to new and better training methods for network administrators. With respect to virtual network training environments, the thesis recommends a new model for cyber situational awareness that is appropriate for use in MAVNATT, as an example of this class of training tool.

II. LITERATURE REVIEW

A. OVERVIEW

Network administrators face numerous challenges in protecting their systems, using tools such as intrusion detection systems, anti-virus applications, or other security sensors to defend against adversaries and to mitigate risks. Cyber situational awareness is not only related to the effectiveness of these tools in protecting these systems, it is also critical to decision makers' ability to understand network contexts and make good tactical decisions (Barford et al., 2010). Many network attacks can be prevented by the configuration of firewalls or null-routing, but these tactics are not sufficient against distributed denial of service (DDOS) attacks (Gray, Ritsos, & Roberts, 2015) or insider threats. By virtue of being inside the secure perimeter, in possession of valid credentials, and having knowledge of the system configurations, insider threats are inherently more difficult to identify than outsider threats (Brancik & Ghinita, 2010). Also, existing system vulnerabilities that were created by programmers during software or system design, either intentionally or not, are a significant industry problem, as they create potential backdoors for external attackers. Moreover, most of these security problems are not found until after a penetration test or, unfortunately, after an attack on the system (Olama & Nutaro, 2013).

Above all, there often exist disconnects between tools and human decision makers (Barford et al., 2010). That is to say, tools can track systems and provide logs to network administrators, but humans still need to decide on the meaning of the data that those tools present (Barford et al., 2010). As new information becomes available, administrators must update their systems, and their knowledge, to mitigate their own vulnerabilities (Tadda & Salemo, 2010).

Although there are many tools for identifying threats and vulnerabilities, the data they provide is often not clear enough for human decision makers to use effectively. These tools may provide large amounts of data, but the network administrator must decide which of the data is meaningful, and whether a vulnerability or threat exists.

Network administrators' situational awareness over the network depends on their ability to make these analyses, given their experience, training, knowledge, and the tools that they use.

The proficiency of network administrators is dependent on realistic experiences. Such experience can be gained in a controlled environment, such as a training lab, or in response to events occurring on the networks for which they are responsible. Hence, the most effective tools, training methods, and best practices should be identified and, where possible, incorporated in an environment capable of enhancing network administrators' situational awareness.

Limited awareness can have a negative impact on an administrator's ability to precisely see multiple threats or adverse activities in parallel. A failure in situational awareness may occur when the measure of information accessible far surpasses an administrator's capacity to process it (Endsley & Connors, 2014).

The administrator's ability to maintain awareness of the state of the system is critical to the security of the system. Thus, an understanding of what is meant by situational awareness in the context of network administration is essential to providing a construct for developing and maturing it.

B. CYBER SITUATIONAL AWARENESS

Incorporating new computer and networking technologies into an existing enterprise means that an organization must be aware of the potential for unexpected effects to the current systems, and thus be prepared to respond to such effects by accumulating a high level of situational awareness (SA) before and after incorporating these changes into the operational network. With increasing cyber threats, any system vulnerability may be potentially exploited, which can result in system failures or information loss. Therefore, building and maintaining SA at every level of the organization is crucial. In particular, administrators of these systems need to be more situationally aware than other users, due to their responsibility to securely protect and maintain network infrastructure and systems.

An essential first step is to define clearly what is meant by *cyber situational awareness* (CSA). This step starts with a review of the basic definition of situational awareness. According to Mica R. Endsley's (1988) definition, "Situational Awareness is 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." As one makes sense of this definition, SA is related to the decision-making process, and thus to decision makers. Moreover, each individual's capability to develop SA varies, as each interprets the same data in a different way due to his natural capacity to understand the data, as well as his education and experience (Endsley, 1995, p. 35). Hence, one can expect different individuals to arrive at different decisions given the same situation and input. Additionally, the presentation of the data will also doubtlessly affect SA (Endsley, 1995, p. 50). While SA tools provide data output to help decision makers, these tools do not ensure that different decision makers will arrive at the same conclusion. According to Endsley (1995), "all system designs are not equal in their ability to convey needed information or in the degree to which they are compatible with basic human information-processing abilities. Other features of the task environment, including workload, stress, and complexity, may also affect SA" (p. 35). Thus, many factors can affect the human decision-making process and the associated situational awareness, which has led many researchers to find novel approaches to help decision makers remain independent of these human factors.

This research uses Endsley's definitions (1988) as well as his model (1995) to reach a clearer understanding of CSA. Endsley (1995) identified three levels of SA: Level 1 SA: Perception of the Elements in the Environment; Level 2 SA: Comprehension of the Current Situation; and Level 3 SA: Projection of Future Status (Endsley, 1995, pp. 36–37). Endsley's model depicting the relationships of the different levels is shown in Figure 1. From this model, we propose corresponding levels of CSA.

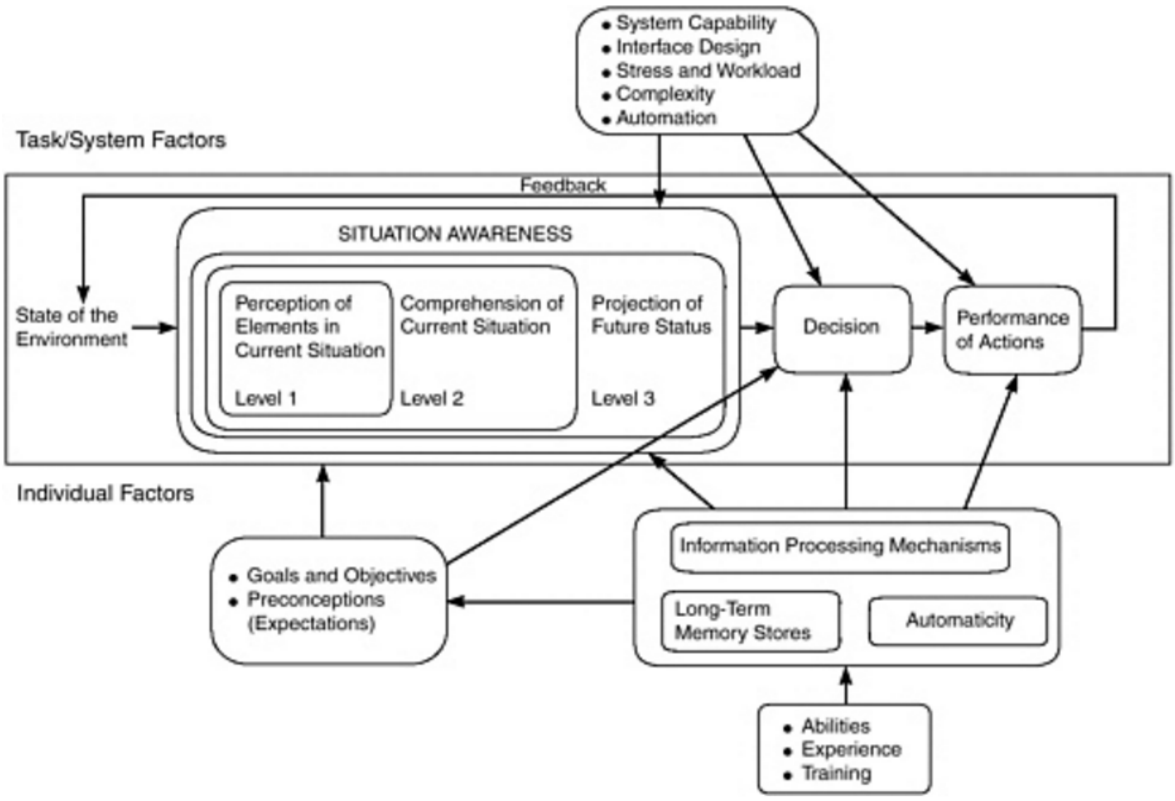

Figure 1. Model of Situational Awareness in Dynamic Decision Making. Source: Endsley (1995).

1. Level 1 SA: Perception of the Elements in the Environment

According to Endsley (1995), "the first step in achieving SA is to perceive the status, attributes, and dynamics of relevant elements in the environment" (p. 36). In the cyber realm, the core concept of this SA level lies in network administrators understanding the basic objectives and elements of the cyber security domain to help them overcome false understanding of their systems' security against cyber-attacks ("Cyber Security Elements," n.d.). The information system security objectives of confidentiality, integrity, and availability (often termed the "CIA triad") (Ross & Swanson, 2004) help to identify conditions necessary to ensure data security; these objectives require that organizations and individuals be alert in monitoring confidentiality, integrity, and availability of their data (Henderson, 2015).

SA over physical systems is developed with respect to the particular techniques and hardware sensors for these systems (Barford et al., 2010). Endsley gives the analogy of an aircraft pilot and automobile driver for explaining level 1 SA. According to these examples, a pilot perceives mountains with the help of aircraft warning lights, while an automobile driver can perceive the location of other vehicles and his car's current status using the automobile's sensor systems (Endsley, 1995). These physical SA systems have slower developing speed than cyber systems (Barford et al., 2010). According to Paul Barford et al., "Cyber SA systems rely on cyber sensors such as IDS', log file sensors, anti-virus systems, malware detectors, and firewalls; they all produce events at a higher level of abstraction than raw network packets" (2010). These CSA sensors provide the necessary information to the administrator, much like the aircraft or automobile warning lights in Endsley's analogies, allowing the administrator to develop an accurate perception of the cyber environment.

In light of the CIA triad, when devising a network security policy, one must be aware of the risks posed by system vulnerabilities and related threats to the system, as well as possible security countermeasures to mitigate these risks (Paquet, 2013). Perception level of awareness covers the cyber sensor's data. Sensor data warns the administrator about the threats and threat indications. These threats may vary from malware to insiders, or social engineering to denial of service (DoS) attacks. According to a Symantec report, over 430 million new unique malicious programs were discovered in 2015, and zero-day vulnerabilities doubled to 54 over the previous year (Symantec, 2016). This finding reveals that cyber security threats are increasing significantly. Of course, knowing about the threats is not enough; an administrator must understand the countermeasures that can be employed against them. For example, developing a strict patch implementation policy may be a good countermeasure for software security risks, while a reliable antivirus detection application and update policy may provide protection against known malware.

Considering the significantly growing numbers of cyber threats and technological developments in computer systems, network administrators must strive to achieve level 1

cyber SA. They must develop their level 1 SA in order to continuously monitor and understand the threat signal data.

2. Level 2 SA: Comprehension of the Current Situation

According to Endsley (1995), "Comprehension of the situation is based on a synthesis of disjointed Level 1 elements." Level 2 SA is about understanding the ongoing situation and its components by using the knowledge of level 1 SA; moreover, interpreting and deciding on it, based on the decision maker's experience and goals (p. 37). Endsley illustrates this level from the perspective of an aircraft fighter pilot: "a military pilot … must comprehend that the appearance of three enemy aircraft within a certain proximity of one another and in a certain geographical location indicates certain things about their objectives" (1995). The network administrator can identify the current situation by assessing the data derived from tools, logs, and sensors to monitor the state of the systems of interest. However, extracting the correct data and identifying the threats still may depend on one's experience and system knowledge since the tools may not recognize new motifs, as previous data or practices may not relate to the current situation (Tadda & Salemo, 2010, p. 23). This level is not only focused on identifying the threats, but also on determining configuration changes, system state changes, or any other changes according to the administrator's goals.

Properly defined goals will help the network administrator better understand information being received, and thus more effectively develop an understanding of the emerging situation (Endsley & Connors, 2014). In this way, the administrators develop an entire picture of the system, which can aid them in recognizing the events pertinent to the system quickly and accurately (Endsley, 1995, p. 37). To illustrate, an unauthorized flash drive insertion alarm from a user's computer does not necessarily indicate an attempt to insert malware into the system intentionally; it may simply indicate an uninformed user regarding the hazards of using a portable flash drive on his or her computer. In another example, friendly-looking emails from an unknown, untrusted source may represent an attempted social engineering attack to the system. Above all, the decision maker is the person who will interpret indications and data based on his goals.

3. Level 3 SA: Projection of Future Status

Endsley (1995) describes the final SA level as "the ability to project the future actions of the elements … achieved through knowledge of the status and dynamics of the elements and comprehension of the situation" (p. 37). This level of Endsley's SA model, before the decision maker propagates the decision, is focused on predicting and determining the future results of the present case to the running system (Endsley & Connors, 2014). Making decisions on possible future results also requires consideration of past experiences, and present outcomes of these experiences (Tadda & Salemo, 2010).

Decision makers must choose the best decision that complies with their purposes in this SA level (Endsley, 1995). Endsley gives another real-world example to demonstrate this: "an air traffic controller needs to put together information on various traffic patterns to determine which runaways will be free, and where there is a potential for collisions" (p. 37). The predictions made at this level are crucial for CSA because the correct evaluation of network events may prevent future cyber-attacks. For example, an attack may be a deception in support of another attack that may bring less indication or warning but carry more effect to the system; or the residuals of this attack may damage the running system over an extended period of time. A clear prediction of potential future impacts may lead the administrator to clean residuals from the operating system or identify new avenues of attack. Therefore, the decision makers responsible for critical and complex systems must have a clear sense of their system objectives rather than simply observe the state of the current situation without an understanding of the impact of such states (Endsley, 1995).

C. MAVNATT

MAVNATT was designed to fill gaps in network administrator training for support to United States Marine Corps tactical networks (McBride, 2015). The goal of the system was to provide a lightweight tool to train network administrators by replicating a tactical network with a virtual network environment. This virtualized environment is intended to replicate the real network to allow administrator training in system implementation, maintenance, and security, since training on the real network

may cause unexpected or detrimental results to that network. If something unacceptable happens in the virtualized environment, it will not impact the mission and does not damage the original network. Moreover, this kind of training may increase the practical experience level of the supported network administrators.

As mentioned in Chapter I, McBride (2015) defined three essential modules comprising the MAVNATT framework and architecture (see Figure 2): mapping, awareness, and virtualization. The framework's goal was to integrate these three modules (McBride, 2015) to allow replication of a real operational network in a virtual network environment.

The MAVNATT framework includes a graphical user interface (GUI) to provide situation awareness for the administrator. This interface provides novice administrators with better SA over a real network and virtualized network, as well as providing for training schema and monitoring of network issues (McBride, 2015).

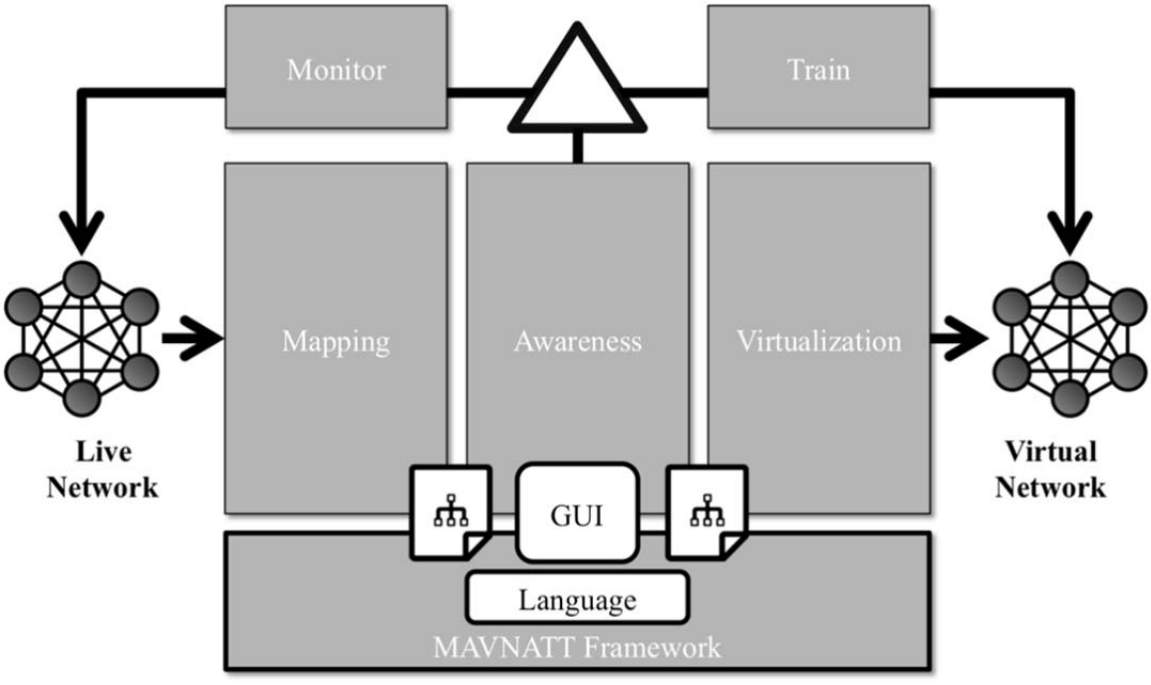

Figure 2. MAVNATT Conceptual Model. Source: McBride (2015).

The MAVNATT GUI must be suitable for showing the real and the virtualized network topologies and easy to learn for users (McBride, 2015). In the MAVNATT technology demonstration, the simplicity of a GUI was able to increase the situational awareness of network administrators, especially for novice users compared to experienced users; novice users need more training due to their lower level of expertise.

As currently defined, the MAVNATT awareness module mostly emphasizes device status within the networks. If a system error happens in a real system, the network administrator must be able to see the same error in the virtual training network. This may help the network administrator work on real network system flaws (McBride, 2015). So, this benefits the system security posture by developing network administrator skills against unexpected situations without harming the mission system. Also, MAVNATT can allow administrators to resolve faults using the virtualized systems or to verify the impact of configuration setting changes, and then apply the solution to the respective real network systems after they have been fully tested in a virtualized environment.

D. SUMMARY

This chapter describes cyber situational awareness and its importance to decision-makers and administrators responsible for critical cyber systems. It further described the purpose of MAVNATT and its awareness module in the context of CSA. By having an understanding of how CSA is established and maintained, developing a methodology for systems like MAVNATT can be possible.

THIS PAGE INTENTIONALLY LEFT BLANK

III. SURVEY OF NETWORK AWARENESS TOOLS AND TECHNIQUES

As mentioned in the previous chapter, cyber situational awareness is a challenging and complex task for human beings. The cyber domain encompasses many components and its events occur very rapidly, making it difficult for the human mind to comprehend; further, events in cyber space may happen in rapid succession. Thus, if an administrator does not have the proper tools and techniques to help protect the cyber system for which he or she is responsible for maintaining and protecting, then successfully accomplishing these tasks is difficult. Furthermore, a lack of appropriate security measures leaves the operating system virtually defenseless against threats. For these reasons, many cyber security professionals maintain a set of security tools, technologies, sources, reports, techniques, and best practices to aid them in securing their cyber systems and environment (Albanese & Jajodia, 2014).

According to Massimiliano Albanese and Sushil Jajodia, a powerful cyber defense framework requires these important functions:

- Learning from attacks
- Prioritization
- Metrics
- Continuous diagnostic and mitigation
- Automation (2014)

Therefore, in this thesis, we consider that people are the ultimate decision makers of automated cyber systems, since they control checking, verifying, and reviewing the results of automated tools (Albanese & Jajodia, 2014). Rather than focus on protocols related to network management in this chapter, we explore some of the critical security solutions related to network administrator techniques and tools to provide a clearer view of CSA.

A. NETWORK SECURITY AND AWARENESS TECHNIQUES

Creating a network requires the physical and logical connection of devices. However, without the correct configuration of devices, physical connections are not enough to build a functioning network, let alone a well-designed and secure network. In fact, there is no perfect cyber system such that its devices work well together forever after initially configuring them. As the network's subsystems, computers, technologies, and software evolve and change, the devices may give errors or their current state may change unexpectedly due to device failure or external action. In addition to changes in device status, attackers may exploit vulnerabilities in misconfigured devices to compromise them until the entire network is eventually compromised. Moreover, if the network operator does not understand what is occurring within a system, or underestimates state changes, the results to the network as a whole may become catastrophic. Further, as the network grows, managing it becomes an increasingly challenging task (McCloghrie & Sanchez, 2001). Therefore, the network's configuration is a critical process which one must always bear in mind.

Management of system configurations is an information technology (IT) area referred to as network configuration management. It is a broad part of network management ("Network Configuration Management," n.d.) and according to Techopedia.com it is defined as

> a broad term for the organization and management of a computer network. All sorts of networks, including local area networks, wireless networks and virtual networks all need elements of maintenance, modification, repair and general monitoring. Network configuration management involves collecting different information about hardware devices, software programs and other elements of the network in order to support administration and troubleshooting. (2016)

This research argues that configuration management can be the first phase of CSA. As discussed in the previous chapter, the first level of SA is "Perception of Elements in Current Situation" (Endsley, 1995). In a cyber network, accurately managing the configuration of the network requires putting together all the pieces of the system to get instantaneous information on the running devices and their current status.

This section covers network security practices for configurations and awareness of Department of Defense (DOD) systems. In the realm of configuration, there are numerous guidelines for configuring systems for computer security best practices, such as Defense Information Agency (DISA)'s Security Technical Implementation Guides, U. S. Government Configuration Baseline, and Center for Internet Security Standards (Byrne, 2015). This thesis discusses only STIGs, since DOD is following this guidance for their cyber systems security. Router access configuration lists are covered as well.

1. Access Control Lists

Access controls lists (ACL) are sets of router-based network traffic filtering rules that provide additional security to networks. ACLs allow a router powerful control over network packets. The router checks inbound and outbound traffic packet headers according to the ACLs; if there was an ACL rule defined for a specific packet, the router decides to permit or deny the actual packet with regard to this rule.

One can create ACLs directly on the router via the command line. For a specific ACL, there will often be more than one rule assigned to that ACL name. On some routers, after assigning rules to an ACL, it is not possible to delete individual rules without deleting the ACL ("Cisco IOS Security Configuration Guide," n.d.). After creating the ACL, one can apply it to the router interfaces based on the interface's connected network; otherwise, the ACL does not run and merely stays in the router's memory.

The order of rules in an ACL is crucial, as the router checks the statements line by line against an incoming packet until a corresponding rule is matched. When the router matches a rule with the packet, it decides to permit or deny the packet based on the rule, and then does not check any remaining rules ("Cisco IOS Security Configuration Guide," n.d.). For instance, if one of the interfaces of the router connects the organization's web server to the network, this interface's ACLs can have rules to permit forwarding of incoming traffic (e.g., allowing incoming connections to port 80) and deny all other inbound packets to that server. This idea is demonstrated by the following example:

access-list sampleRule permit tcp 20.3. 9.0 0.0. 0.255 any eq 80

access-list sampleRule deny ip any any

Ordering of rules is also critical with regard to rule types. For example, if a network administrator defined permit rules after the deny rules, no traffic could access a web server. Although this is a very simple example of misconfiguration, and one that can easily be detected and fixed, there might be more complex ACLs where errors in configuration could cause serious network traffic degradation or failure. Detection of such errors may take significant time. Due to human error in ACL configurations, the system state can become invalid; moreover, these systems may become vulnerable to cyber-attacks. According to Nancy Navato (2001), these errors are "failure to create and add access list entries in the correct sequence," "failure to apply the access list to an interface in the correct direction," and "failure to apply the access list to an interface." Hence, network administrators should be careful when creating ACLs. After creating ACL lists, network administrators must also on occasion review them to ensure the ACL lists are still current (Navato, 2001).

2. Security Technical Implementation Guides

Security Technical Implementation Guides (STIG) are configuration documents that explain how to configure various computing and network devices to mitigate security risks (Byrne, 2015). According to the DISA webpage, "STIGs contain technical guidance to 'lock down' information systems/software that might otherwise be vulnerable to a malicious computer attack" ("STIGs Home," n.d.). DISA has defined more than 400 STIGs for different types and versions of software and systems. The DISA STIGs website allows the public to download STIG zip files, where one zip file may contain pdf archives and a STIG folder, or it may contain only a STIG file. These pdf archives can give unclassified information about the overview of the downloaded STIG, its revision history, and Security Requirements Guides about the technology related to the STIG. Every STIG is categorized according to the DISA guidelines shown in Table 1.

Table 1. Vulnerability Severity Category Code Definitions.
Source: "STIGs Home" (n.d.).

DISA Category Code Guidelines	
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the exploitation of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

Additionally, most STIGs are in Extensible Markup Language (XML) format, for which DISA has a useful STIG Viewer java tool that allows viewing of STIG files more easily. This tool has the ability to show more than one STIG, as well as to filter responses according to severity categories or keywords. An example of this is shown in Figure 3, where this research imported Apple iOS 10, Microsoft Word 2013, Application Layer Gateway, and Apache Server 2.2 technical guides to the DISA STIG Viewer.

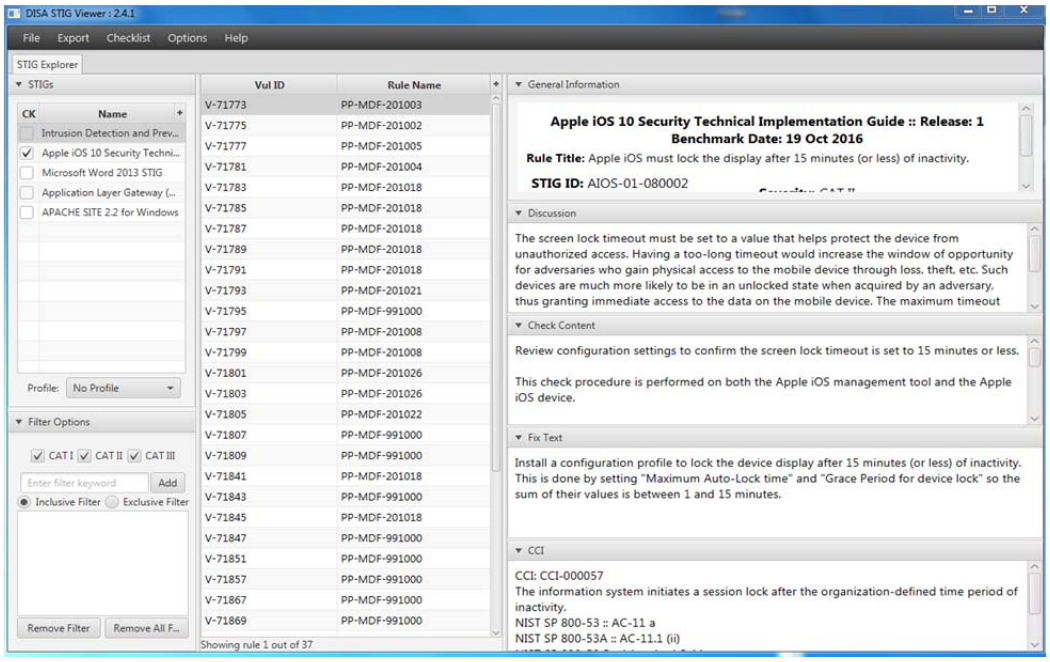

Figure 3. DISA STIG Viewer

Although STIGs are prepared to secure DOD infrastructure, anyone can freely access and implement these policies for the own organization. However, before changing any software configuration, one should take into consideration that the updated security settings of one application may affect other applications' security settings or state. Therefore, network administrators are responsible for adapting the STIG guides to their systems by considering the effects of the policies. Such adaptation requires significant understanding of the system for which the administrator is responsible, an understanding only developed through significant practice and operational experience.

3. System Logs

According to Karen Kent and Murugiah P. Souppaya (2006), a log is "a record of the events occurring within an organization's system and networks" (p. 2–1). Logs may pertain to hardware devices, software, services, databases, or operating systems. Logging mechanisms can serve as a feedback mechanism to generate positive information about the state of the system; they can also serve as an alert system to inform the network operators regarding a critical situation. Oftentimes, being notified of and analyzing the errors on a system, or getting real-time information about running software, may not be possible without continuous logging mechanisms in place on that system.

Furthermore, the requirements of network management make logging inevitable. Routine log surveys and examination are essential for recognizing network problems, security incidents, policy abuses, and criminal activity after they have happened (Kent & Souppaya, 2006). Different systems may use different vendor-based logging formats; therefore, in order to review all logs in human readable format, organizations usually require changing the various logs into a common format (Kent & Souppaya, 2006). In these circumstances, log management tools can help to eliminate different formats and show human readable logs to the network administrators.

Also, logging can provide information to identify unauthorized data breaches. For example, an organization creating web applications for its departments might use the real databases rather than test databases for software test and development purposes, giving database access permission to their software programmers. In that situation, database

query logs can show *how* the software developers are engaging with the database, and who among them may be abusing their authority on the system as a potential insider threat.

B. NETWORK AWARENESS TOOLS

Considering the volume and velocity of network traffic in modern cyber systems, administrators of these systems must rely on sensor data to develop CSA, as described in Chapter II. Using tools that can provide more actionable and human readable data to network administrators is very important. There are many network monitoring and assessment tools available commercially, with varying prices and capabilities. It is not possible to evaluate all of these tools in this research; therefore, this research describes some of the configuration and cyber security tools that relate to and support CSA.

1. Firewalls

A firewall is a network security device or a host-based application that monitors network traffic flow, then blocks or filters incoming and outgoing traffic (packets) according to predefined filtering rules (West, Dean, & Andrews, 2015, p. 405). For instance, the Windows operating system comes with an integrated host-based Windows Firewall. Furthermore, anti-malware tools may also contain a firewall that is integrated within the application. Those are examples of host-based firewalls that protect the personal computers or servers on which they are loaded.

Protecting the entire network, however, requires network-based firewalls. These firewalls are installed at the entrance to the network as a course filter to protect the network from any externally-induced malicious network behavior. Routers are one example of network-based firewalls since they have the ability to perform packet filtering (Northrup, n.d.). Although network firewalls may come preconfigured to prevent most common typical security threats, network administrators may customize the firewall settings in accordance with their network needs (West et al., 2015, p. 406).

Packet filtering is not the only benefit of network-based firewalls. There are different firewalls that have functionality to strengthen network security, such as logging,

encryption, and user authentication (West et al., 2015, p. 407). Since firewalls do not block all malicious traffic on a network, a logging capability can help the network administrators develop CSA; for example, logs may be reviewed after a security breach to analyze the attacker's behaviors or to get a clearer view of how the attacker managed to pass the firewall to gain access to the system (Northrup, n.d.). This data may help network administrators to change security configurations by adding new rule sets to the firewall settings.

2. Intrusion Detection Systems

An intrusion detection system (IDS) is a software or hardware device that monitors network traffic and produces alerts when a potential network security incident occurs (West et al., 2015, p. 402). The main goal of an IDS is to recognize potential network security events (Scarfone & Mell, 2007). Accordingly, an IDS has nothing to do with prevention of an intrusion, but rather it raises alerts and logs the detection of an intrusion. Thus, an IDS provides necessary information to the network administrator by logging all probable incidents, allowing the administrator to take actions to mitigate the effects of the potential attack (Scarfone & Mell, 2007).

IDS systems work like a network sniffer, capturing and analyzing packets as they traverse the network. Understanding the security incidents from the captured network traffic requires extra effort, as well as practice, for a security analyst. However, an IDS not only captures the network traffic, it can examine the traffic from the standpoint of network security (Snyder, 2009). Therefore, IDSs can be tailored to adopt various techniques to detect the security issues. An IDS can be configured to utilize several different methods of detection, such as signature-based or anomaly-based, or through stateful protocol analysis (Scarfone & Mell, 2007).

Signature-based detection uses the same approach to detection as anti-virus software, so that the IDS compares captured traffic to samples in its database and attempts to match the known attack vectors with the observed network packets (Bradley, 2016). However, this approach may be inefficient against any unknown or new security

threats, such as zero-day attacks, whose presence is hidden until the intended “release date.”

Anomaly-based detection is a very powerful method to help administrators become aware of any new kind of attacks. Anomaly-based IDSs observe the network over time to create a characterization of the network’s “normal” behavior. Then they compare the learned behavior with the current state of the network to find significant changes or anomalies in traffic patterns and characteristics (Scarfone & Mell, 2007).

Stateful protocol analysis is an entirely different approach that depends on IDS vendor-specific configurations as to how the exact protocols should behave in the system (Scarfone & Mell, 2007). For instance, according to this method the IDS may alert any connection to port 4444; because Metasploit, a common hacking tool, often uses port 4444 as a default, it is highly likely that the IDS system will detect and alert this action as potential exploitation or malicious activity. Moreover, network administrators can also create their personal security rules according to their network protection concerns regarding their cyber environments.

In addition to the detection methodologies discussed earlier, there are two categories of IDSs: host-based (HIDS) and network-based (NIDS). As one can assume from its name, HIDS operates on a single machine in order to protect that system. Most probably, this machine is a critical server for the organization, so one may need to analyze significant security incidents occurring on that server by looking at that machine’s HIDS logs. NIDS, conversely, protect a network by running on a critical edge of the network so it can monitor all incoming and outgoing traffic (Bradley, 2016), as well as traffic internal to the network. However, placing only one NIDS for an extensive network may have undesirable side effects for the network. To illustrate, if the monitoring capacity of the NIDS is lower than the flowing traffic, it may miss important security issues; so, it may not alert for all detectable events. Eventually, this kind of installation on a large capacity network may leave the system vulnerable because it does not provide enough data to the network administrator. Therefore, one should use more than one NIDS in series, as necessary, on a larger-scale network. For example, if the

system consists of a wireless network with a demilitarized zone, installing two different NIDSs for each of those networks may increase the network monitoring capacity.

3. Intrusion Prevention Systems

Intrusion Prevention Systems (IPS) are powerful tools in that they not only have the ability to operate with the same logic as IDSs, but also can prevent intrusion incidents from happening. There are different types of IPSs with different capabilities to prevent attacks. With respect to these capabilities, an IPS can prevent attacks by ending a connection or user session, changing the security configurations of the system, or changing malicious content (Scarfone & Mell, 2007). For example, an IPS can scan incoming emails and remove any malicious attachment, then permit the email to reach its receiver without the harmful attachment (Scarfone & Mell, 2007).

System administrators can use IPSs in conjunction with IDSs. This decision depends on the organization's network security policies. However, IPSs may provide robust security tools for the network security. Due to their capability for prevention, they make it less difficult for the network administrators to secure their systems. Obviously, some threats may pass through the systems' prevention mechanisms; however, reducing the number of threats inside the system can help network administrators concentrate on the security issues that exist within the network.

4. Anti-Virus Software

Anti-virus (AV) or anti-malware software can protect systems against malicious software by using signature- or behavior-based database definition comparisons. Anti-virus software has a predominant role in the protection of organizational networks. Even though they do not have the ability to find malware that does not contain a signature present in their database, AV systems can prevent critical known security issues that may occur on a host. For instance, an end-user who does not know basic computer security may insert a flash drive that contains malware into the organization's computer that does not have any anti-virus protection, which may result in that malware spreading through the system. However, if the system had host-based AV software installed, it could detect and eradicate the virus.

There are many kinds of AV software available with different features. For this reason, network security administrators should carefully choose the proper software for own organizational needs. According to Jill West et al., (2015), AV software should have at least these capabilities:

- Detect malware through signature scanning
- Detect malware through integrity checking
- Detect malware by monitoring unexpected file changes or virus-like behaviors
- Receive regular updates and modifications
- Consistently report only valid instances of malware (p. 418)

All of those features can help make the system more secure against malware. Still, end-user awareness plays a major role in malware protection. For instance, an attacker can conduct a social engineering attack on the organization's employees by sending brand-new malware as an attractive email attachment. Accordingly, even the best signature-based AV software cannot detect this malware. Even if only one person opens that attachment, the network administrator's efforts to secure the network go for naught.

5. Nagios XI

Nagios XI is a Linux-based tool that contains many features benefiting IT infrastructure and managers by monitoring necessary elements of the network. Robust dashboards give initial access to observe the data effectively. Users can customize the layout, preferences, and design according to personal choice ("Nagios XI," 2016). To increase awareness, Nagios XI may send outage details via email or mobile alerts to the responsible personnel so that they can solve the problem at once ("Nagios XI," 2016). Figure 4 shows one of the Nagios XI features, an example of a network replay report, which shows the network devices' status over time. The interactive nodes in this figure allow the network administrator to understand the historical status of each device ("Nagios XI," n.d.).

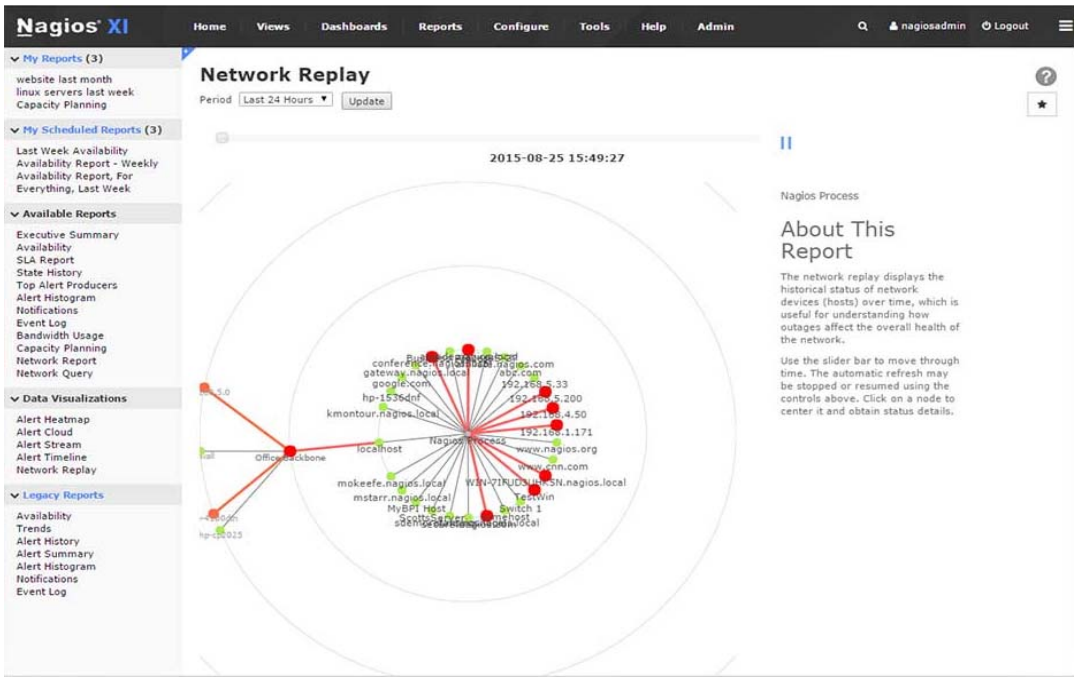

Figure 4. Nagios XI Infrastructure Management Feature, Example of Network Replay Report. Source: "Nagios XI" (2016).

Nagios XI also has a powerful monitoring engine that allows users active and extended monitoring. Also, the tool has a web interface and provides advanced graphs to increase user visibility into the system state. Specifically for convenient configuration of the network devices, Nagios XI provides Configuration Wizards to easily set up devices, services, databases and so on ("Nagios XI," 2016).

6. NetCrunch

NetCrunch is a high capacity network-monitoring tool that is able to detect network devices automatically, identify the device type, or find out whether the device supports SNMP, Simple Network Management Protocol (*NetCrunch*, n.d.). Accordingly, NetCrunch can automatically build routing, logical network, and Data Link Layer (Layer 2) maps (*NetCrunch*, n.d.). For managing network devices, NetCrunch uses SNMP (*NetCrunch*, n.d.). NetCrunch also has many capabilities, such as traffic monitoring from different flow sources, log monitoring, hardware and software inventory by which the software can show data about installed patches, and alerting abilities (*NetCrunch*, n.d.).

NetCrunch can run 56 previously defined actions on remote hosts, such as rebooting machines or restarting services (*NetCrunch*, n.d.). This program also uses an alert notification system via email or text messages (*NetCrunch*, n.d.). Correspondingly, it shows current alerts in the "Pending Alerts View" screen so as to draw the attention of the users to present network problems rather than having to look through the event logs only (see Figure 5).

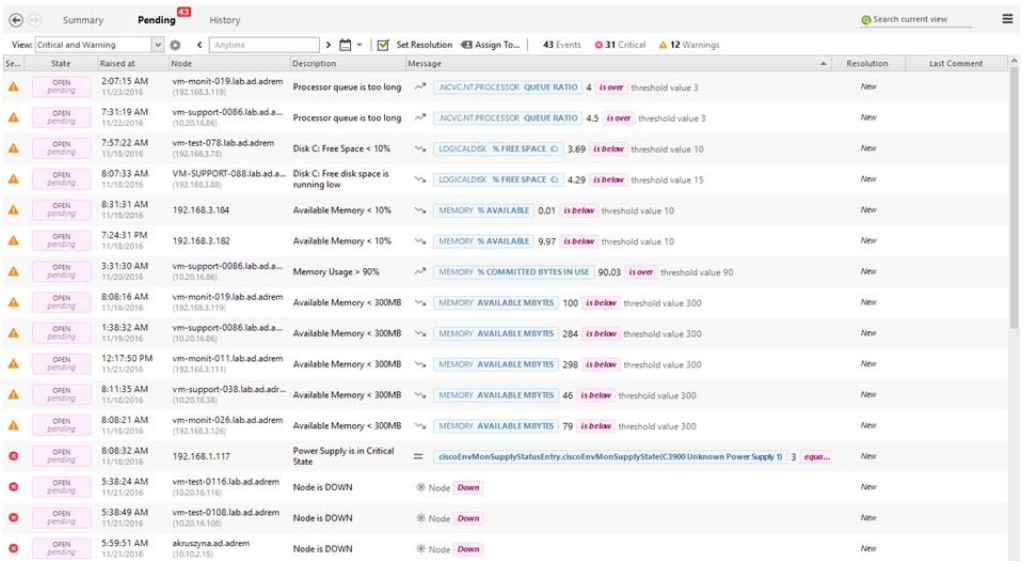

Figure 5. NetCrunch Pending Alerts View, Example Display. Source: "NetCrunch" (n.d.).

7. Solaris Network Performance Monitor

Solaris Network Performance Monitor (NPM) is a Windows-based network monitoring and management software product. It has powerful features that may help network administrators increase their situational awareness of the network devices. According to Solaris NPM website, some of the features of the software are:

- Customizable topology and dependency-aware intelligent alerts
- Dynamic wired and wireless network discovery and mapping
- Automated capacity forecasting alerting, and reporting
- Wireless network monitoring and management

- Consultant-and services-free deployment
- Customizable single-pane-of-glass network monitoring software
- Hardware health monitoring and alerting
- Customizable performance and availability reports
- Dynamic statistical network performance baselines (“SolarWinds,” n.d.)

Monitoring different kinds of devices with the help of these abilities, a network administrator may have sufficient information about the current situation of the network to respond quickly to network troubles that arises.

Also, as shown in Figure 6, the ability to group network nodes by vendor can provide further information to the administrator as to whether the detected problem that requires attention might be a product-based issue (“SolarWinds,” n.d.). To illustrate, if one of a vendor’s products starts to send more errors, this may be the result of a vulnerability or the result of a vendor-released patch that is not compatible with the system.

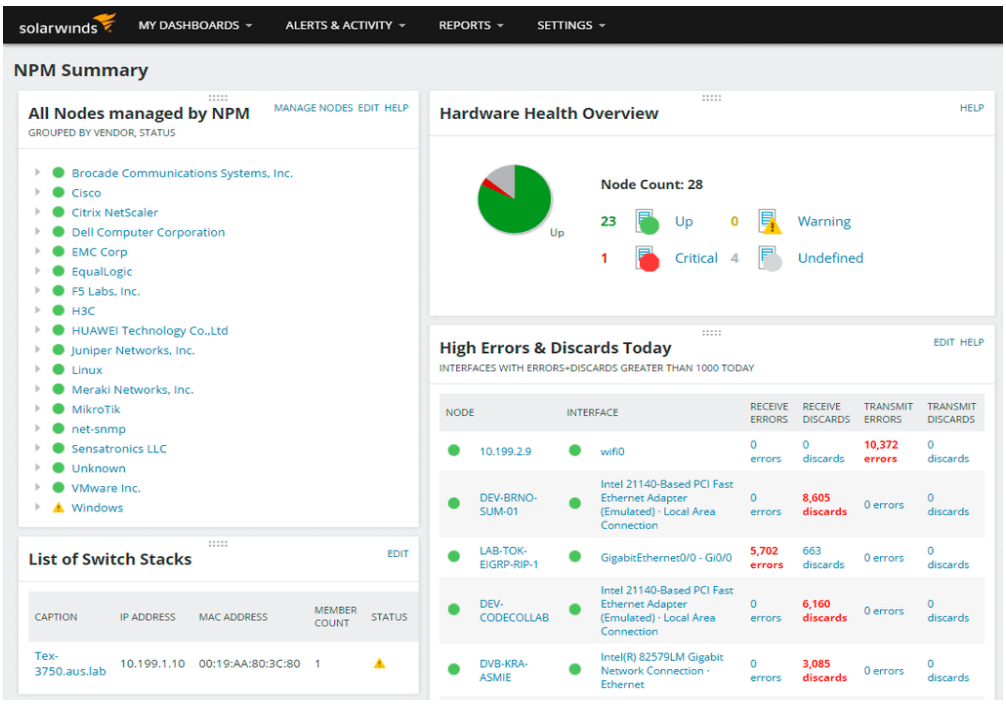

Figure 6. Solaris NPM Network Availability and Performance Monitoring Screenshot. Source: “SolarWinds” (n.d.).

8. Host Based Security System

The Host Based Security System (HBSS) is a DOD program. According to Mike Gawlas (2009), the main goal of this program is "to provide network administrators and security personnel with mechanisms to prevent, detect, track, report and remediate malicious computer-related activities and incidents across all Defense Department networks and information systems" (Gawlas, 2009). Thus, HBSS can enhance CSA of DOD systems by strengthening its command and control over the associated cyber systems (Boland, 2012).

HBSS is a combination of the network and host based security systems employed by the DOD for each host on the controlled networks (Boland, 2012). The system has the ability to allow the use of only authorized software and devices on the network in accordance with the predefined rules (Gawlas, 2009). HBSS has many capabilities to maintain host security, such as the ability to check a host's behavior by comparing the common behaviors of the host with the current authorized behavior so that the system generates an alert regarding an unexpected activity (Newth, 2016).

C. SUMMARY

The goal of this chapter was to develop an understanding of the types of tools and techniques necessary and available to build and maintain secure networks. Herein it was discussed that all of the cyber security techniques and tools presented are helpful to protect the associated networks and devices, as well as to develop CSA. Better CSA serves to strengthen the security of the cyber systems. The next chapter proposes a design model for network administrators to develop and maintain CSA using the tools and techniques presented in this chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. CYBER SITUATIONAL AWARENESS MODEL DESIGN

Access to data is becoming more and more digitalized, however, the rapid increase in volume of digital information used by commercial and government enterprises has necessitated new, more robust, and powerful information systems to store, process, and analyze this data. Hard disks, software, computer processors, and other computer technologies are growing rapidly in order to handle and store all this emerging data. New technologies and systems continue to appear, such as cyber-rich networks, cloud environments, the Internet of Things, artificial intelligence, and so on. As users' data requirements grow more complex, they demand information-dependent technologies that are interdependent with one other. At the same time, this growth in data systems technology is also placing greater demands on security to protect the valuable data within these systems. The transportation, maintenance, and protection of such data require significant resources. Automation processes and tools are being leveraged by enterprises to address these requirements by using similar information technologies to analyze the data of interest. However, the complexity of the automation processes themselves also produces more raw data to be assessed by human decision makers, inevitably adding to the complexity of the network administrator's role. It is critical that enterprises have complete and accurate situational awareness of their systems to support to proper decision making.

As discussed in Chapter II, CSA is of crucial importance to securing cyber systems. Most CSA tools help cyber security professionals by initiating alerts, warning messages, and log entries, while some tools, like IPSs, protect the systems themselves against cyber threats. However, security reports such as Symantec's 2016 *Internet Security Threat Report* show that security threats are not decreasing with respect to the bulk of the tools. Instead, the number of threats is significantly increasing.

Oftentimes, an expert cyber security professional is effectively a novice user when a new technology is introduced. Developing CSA by utilizing tools remains limited without enhancing human understanding. This requires users to continuously cultivate and maintain CSA.

Making decisions based on sensor data is necessary to protect cyber systems; however, this is not always sufficient. Since a cyber system may consist of many entities, focusing on it as only one entity is not sufficient. Yet, the complexity of the integrated cyber systems within a network does not lend itself to discussion that treats each component separately. Accordingly, understanding a complex system by dividing it into its hierarchical elements might yield more timely and accurate decisions. Therefore, to develop better CSA of cyber networks and systems, one should start by understanding them from end-to-end by developing a new CSA model.

A. CYBER SITUATIONAL AWARENESS PYRAMID

Considering the importance of CSA with respect to the decision-making process, it is clear that it should be analyzed from multiple, hierarchical perspectives regarding cyber security. Just as dividing systems into different components reduces their complexity, using an incremental approach to CSA may help to reduce the logical complexity of the cyber systems of interest, thus improving our understanding of these components parts and contributing to improved CSA.

We define CSA as being composed of configurational awareness, operational awareness, and special conditions awareness. If one can clearly identify and implement the goals of each of these parts of a cyber system, one can approach absolute awareness of cyber security. The component parts of CSA are hierarchical in their nature, and can be envisioned as a pyramid, as shown in Figure 7.

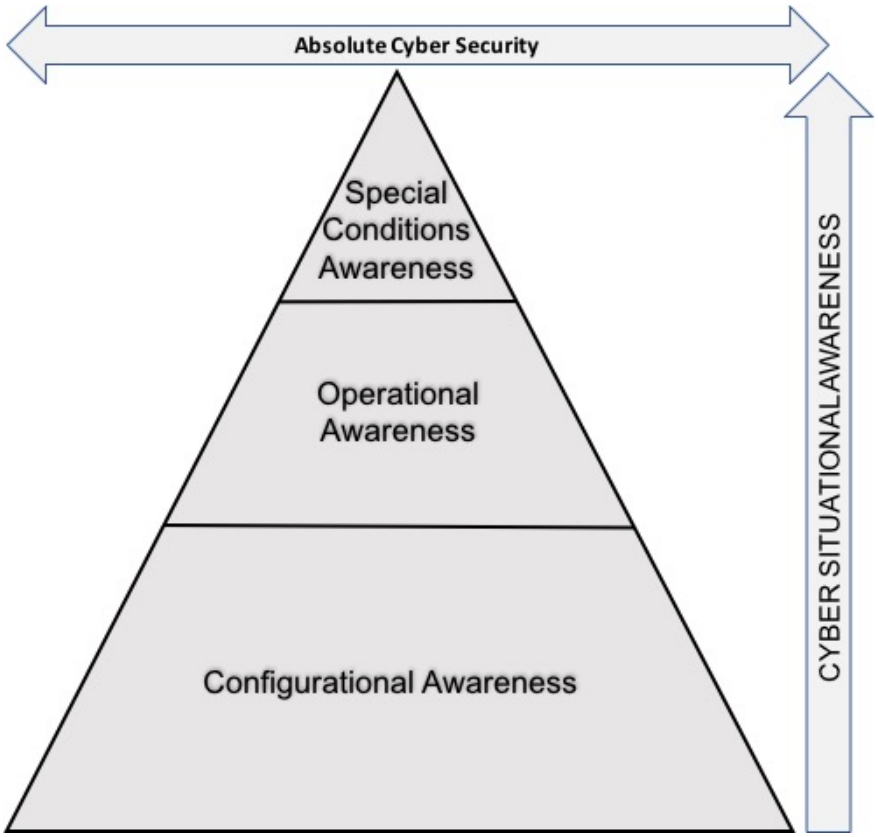

Figure 7. Cyber Situational Awareness (CSA) Pyramid.

As each level of the pyramid is accomplished well, the administrator's CSA increases, reducing the logical complexity of the system. This then allows the decision maker to focus on the next level. Finally, reaching the top level, the administrator may achieve maximum CSA of the system. Without achieving the lower levels, it is not possible to develop CSA at the next level. When a lower level has unresolved problems associated with it, the administrator will be unable to identify or resolve problems associated with the next level.

1. Configurational Awareness

Configurational awareness (CA) is the base of the CSA pyramid; it represents the reality that the configuration is the foundation of information system security. Without a proper configuration policy, maintaining secure and reliable cyber systems would not be

possible. Building better configuration management of a system reduces the security risks to that system.

As discussed earlier, CSA depends on the data that sensors produce continuously. Sensors tend to produce more data in a poorly configured system than they do in a well configured one; for example, a system without a proper configuration easily becomes vulnerable. This tends to increase false positive sensor data, such as with IDSs, which can lead administrators to make poor decisions as they could miss critical valid data due to the complexity and chaos of the information being received. Eventually, this overload of invalid data due to poor system configuration results in the administrator's CSA decreasing dramatically. However, in a converse scenario, an administrator of a well-configured system does not have to cope with configuration-related data. When the system is properly configured according to best practices, the administrator is able to focus on the operational level of awareness because the system's configuration generates less distracting invalid sensor data. Thus, it is easier for the network administrator to comprehend the activity of the network associated with operations.

Sometimes well-configured networks can also have problems caused by human errors introduced to the configuration process. The solution to this problem is to monitor the system configuration by implementing network configuration management tools. These tools not only provide necessary information about the system configuration but also help to configure all of the network devices, thus enabling administrators to focus on the upper levels of the CSA pyramid.

2. Operational Awareness

Cyber security must continuously identify each threat, block each threat, and then address the vulnerability that is the root cause of the risk associated with the threat. In the operational awareness (OA) level of CSA, cyber security tools help to identify threats to the system. Tools such as IDS, firewalls, or anti-virus software provide operational warnings and log entries while the system is in operation. Threats identified by such tools help the administrator eliminate and block these threats. The administrator may do this by deleting malicious software, blocking an IP address, or changing the configuration of the

system. This threat detection and prevention is a continuing process, depending on the emergence of threat during the system's operation.

As described in the CA component of CSA pyramid, administrators of a well-configured system can more effectively focus on the most critical issues in OA. Automation plays a critical role in accomplishing this in OA. Correctly configured IPSs, or other cyber security automation tools, may do a significant portion of the job without human interaction. So, the administrator can focus on more relevant and critical sensor data to analyze it in terms of cyber security. Thus, automation helps to decrease the amount of unnecessary data requiring manual inspection. Though these tools may come with a default set of configurations, they still require custom configuration with respect to the system they support and for expected or emerging threat patterns. Eventually, a proper and accurate configuration of these tools enhances system security by supporting the administrator's OA.

3. Special Conditions Awareness

The CA and OA components of CSA focus primarily on administrator level CSA. One should not neglect, however, the user level of awareness as being critical to overall CSA; this user level is captured by special conditions awareness (SCA). SCA is the uppermost level of the CSA pyramid, as without CA and OA the network administrator may not be able to detect risk behaviors by system users, such as inserting unauthenticated removable media into system devices or attempting to install suspicious and unnecessary software. Even correctly configured and protected systems might be compromised if this level of CSA is not achieved.

It is not possible to define all of the special conditions that might expose a cyber system to attacks or persistent threats because, as the systems evolve, new threats may appear. Even the best cyber security tools that focus on CA and OA may not be able to identify all types of threats that may appear to the user system; thus, there is no absolute cyber security level achieved without developing and maintaining user level CSA. To illustrate this point, consider a secure network in which security tools and techniques are employed to protect its perimeter. Even a system like this may not be entirely secure, as

human users are utilizing the system. An aggressive, well-structured phishing attack may result in even a trained user dropping his guard and releasing information to the attacker that could result in system compromise.

Curiosity, desires, and other behaviors associated with human nature make cyber systems vulnerable to insider threats. However, if users with higher CSA realize something is happening within their cyber environment and report suspicious activity to the administrators, these users can make a real difference in the overall security of the system. So, even non-expert users receiving security-related training and experience is as vital as properly trained system administrators.

B. SUMMARY

This chapter has presented a model of cyber situational awareness based on a pyramid concept of interrelated levels of SA for cyber systems and the networks that they protect. The model suggests that three hierarchical levels of SA contribute to developing better CSA. The model divides CSA into three distinct levels to better understand, maintain, and improve awareness over networked systems. These levels are configurational awareness, operational awareness, and special conditions awareness. Without achieving awareness at the lowest level of the model, the administrator will have difficulty improving the upper levels of awareness. Therefore, these levels of awareness must be achieved from the bottom up to affect the network administrator's CSA. Achieving all levels of the CSA pyramid directly supports the goal of achieving absolute security in cyber systems.

V. CONCLUSION AND FUTURE WORK

A. SUMMARY AND CONCLUSION

The purpose of this research was to understand cyber situational awareness with regard to the perspective of network administrators, to help shed light on the requirements of training for cyber security professionals. The research argued that improving administrators' CSA may help to better secure cyber systems. Continuous monitoring of cyber systems is critical to achieving that goal. To this end, administrators benefit from informed, experienced use of available network tools and best practices and techniques.

To promote the understanding of CSA, this research first discussed the concepts of situational awareness as they pertain to management and use of cyber systems. Next, the research surveyed some of the tools and techniques pertinent to generating CSA. Finally, the research proposed a CSA development model in order to guide the establishment and maintenance of effective CSA of network administrators and users whose principal responsibility is the operation of cyber systems.

There are many cyber security and network monitoring tools available, each with many different features. Some enhance cyber system oversight by automatically detecting or preventing external attacks and reducing the number of threats to reach the inside of the systems. Still, these do not provide enough protection against novel threats, which are the most dangerous ones. Such threats require human analysis of the sensor data. Additionally, cyber security and network monitoring tools may produce significant volumes of data, potentially more than the human brain can effectively comprehend. The velocity of the data also makes it more difficult to maintain awareness of the critical cyber security data inherent in a complex system with complex data.

The research aimed to decrease this complexity by proposing the CSA pyramid. This pyramid consists of three levels, depicting a hierarchy of addressing security threats: configurational awareness, operational awareness, and special conditions awareness. These levels of awareness, addressed from bottom to top, seek to improve system

administrators' CSA. The ultimate goal of this model is to support the achievement of absolute cyber security through human interaction with proper security tools and techniques. Also, the research concludes that administrator CSA is not enough for absolute security; system user CSA also must be supported by the model. This result shows that continued user training is as critical to system security as is network administrator training.

B. FUTURE WORK

The research benefits the MAVNATT awareness module by defining CSA and a model that may guide the development of both administrator and user CSA. MAVNATT does not currently have an awareness module implemented. Additional research may build this module for MAVNATT by employing the proposed CSA model.

Using machine learning to automate threat protection processes may help to develop a more secure cyber system by enabling administrators to focus may effectively on the higher levels of CSA. Conducting research to implement machine-learning algorithms as new tools for the generation of CSA may improve the cyber security of systems of interest. Further, artificial intelligence is a powerful concept in information technology. Therefore, new research should look into how to use artificial intelligence to develop CSA.

Human interaction with cyber systems is not making networks and their components safer. User activities, such as unwittingly opening email attachments or using flash drives containing malware, are some of the causes of cyber-attacks. Reducing human interaction by implementing virtual systems, such as that envisioned by MAVNATT, may reduce risks introduced by system users. Therefore, host-based systems that examine the data in a virtual environment before opening it in the real environment may reduce the security risks by increasing the user's understanding of the potentially catastrophic effects of poor cyber situational unawareness. Research into this area can make a real difference in overall network security.

CSA training is becoming compulsory in many critical organizations. Research about how to test the effectiveness of this training may help to improve current training methods.

Information technology is significantly evolving as discussed in this research. The Internet of Things (IoT) is an example of this evolving technology. As IoT poses increasing vunerabilities to established systems by presenting new vectors of exposure, the security of IoT also presents increased cyber security concerns; it poses new opportunities to conduct research about configurational and operational awareness of CSA.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Albanese, M., & Jajodia, S. (2014). Formation of awareness. In A. Kott, C. Wang, & R. F. Erbacher (Eds.), *Cyber defense and situational awareness* (pp. 47–62). Springer International Publishing. Retrieved from http://link.springer.com/chapter/10.1007/978-3-319-11391-3_4

Barford, P., Dacier, M., Dietterich, T. G., Fredrikson, M., Giffin, J., Jajodia, S., … John, Y. (2010). Cyber SA: Situational awareness for cyber defense. In S. Jajodia, P. Liu, V. Swarup, & C. Wang (Eds.) *Cyber situational awareness* (pp. 3–14). New York: Springer.

Boland, R. (2012, August). Securing military devices. *SIGNAL Magazine*. Retrieved from http://www.afcea.org/content/?q=securing-military-devices

Bradley, T. (2016). Everything you need to know about Intrusion Detection Systems (IDS). Retrieved January 12, 2017, from https://www.lifewire.com/introduction-to-intrusion-detection-systems-ids-2486799

Brancik, K., & Ghinita, G. (2010). The optimization of situational awareness for insider threat detection. https://doi.org/10.1145/1943513.1943544

Byrne, D. (2015). Beyond compliance: DISA STIGs' role in cybersecurity. Retrieved January 2, 2017, from https://gcn.com/articles/2015/05/14/disa-stig-compliance.aspx

Cisco IOS Security Configuration Guide, Release 12.2—Access Control Lists: Overview and Guidelines [Cisco IOS Software Release 12.2]. (n.d.). Retrieved January 8, 2017, from http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacls.html

Configure commonly used IP ACLs—Cisco. (n.d.). Retrieved February 16, 2017, from http://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html

Cyber security elements – Vital for data protection. (n.d.). Retrieved November 20, 2016 from http://www.crossdomainsolutions.com/cyber-security/elements/

Endsley, M. R. (1988). Situation awareness global assessment technique (SAGAT). In *Aerospace and Electronics Conference, 1988. NAECON 1988. Proceedings of the IEEE 1988 National: Vol. 3* (pp. 789–795). https://doi.org/10.1109/NAECON.1988.195097

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, *37*(1), 32–64. https://doi.org/10.1518/001872095779049543

Endsley, M. R., & Connors, E. S. (2014). Foundation and challenges. In A. Kott, C. Wang, & R. F. Erbacher (Eds.), *Cyber Defense and Situational Awareness* (pp. 7–27). Springer International Publishing. https://doi.org/10.1007/978-3-319-11391-3_2

Gawlas, M. (2009, April 15). End-point security spreads throughout military. *SIGNAL Magazine*. Retrieved January 16, 2017, from http://www.afcea.org/content/?q=end-point-security-spreads-throughout-military

Gray, C. C., Ritsos, P. D., & Roberts, J. C. (2015). Contextual network navigation to provide situational awareness for network administrators. In *Visualization for Cyber Security (VizSec), 2015 IEEE Symposium on* (pp. 1–8). https://doi.org/10.1109/VIZSEC. 2015.7312769

Henderson, A. (2015, July 5). The CIA Triad: Confidentiality, integrity, availability. Retrieved from http://panmore.com/the-cia-triad-confidentiality-integrity-availability

Kent, K., & Souppaya, M. P. (2006). *SP 800–92. Guide to computer security log management*. Gaithersburg, MD: National Institute of Standards & Technology.

McBride, D. C. (2015). *Mapping, awareness, and virtualization network administrator training tool (MAVNATT) architecture and framework* (Master's thesis). Retrieved from Calhoun http://calhoun.nps.edu/bitstream/handle/10945/45900/15Jun_McBride_Daniel.pdf?sequence=1&isAllowed=y

McCloghrie, K., & Sanchez, L. A. (2001). Requirements for configuration management of IP-based networks. Retrieved December 27, 2016, from https://tools.ietf.org/html/rfc3139#section-4.0

Nagios XI—Easy Network, Server Monitoring and Alerting. (2016, February 1). Retrieved from https://www.nagios.com/products/nagios-xi/

Nagios XI—Reports. (n.d.). Retrieved February 16, 2017, from https://support.nagios.com/kb/article.php?id=23

Navato, N. (2001). Easy steps to Cisco extended access list. Retrieved from https://www.sans.org/reading-room/whitepapers/networkdevs/easy-steps-cisco-extended-access-list-231

NetCrunch Product Datasheet & Specification. (n.d.). adrem software. Retrieved December 28, 2016 from https://www.adremsoft.com/netcrunch/monitoring/datasheet

Network configuration management. (n.d.). Retrieved December 26, 2016, from http://www.cisco.com/en/US/technologies/tk869/tk769/technologies_white_paper0900aecd806c0d88.html

Network monitoring software | SolarWinds NPM 12. (n.d.). Retrieved January 1, 2017, from http://www.solarwinds.com/network-performance-monitor

Newth, A. (2016, December 16). What is a host-based security system? Retrieved January 16, 2017, from http://www.wisegeek.com/what-is-a-host-based-security-system.htm

Northrup, T. (n.d.). Firewalls. Retrieved January 6, 2017, from https://technet.microsoft.com/en-us/library/cc700820. aspx

Olama, M. M. & Nutaro, J. (2013). Secure it now or secure it later: The benefits of addressing cyber-security from the outset (Vol. 8757). doi: 10.1117/12.2015465

Paquet, C. (2013, February 5). Network security concepts and policies. Retrieved November 21, 2016, from http://www.ciscopress.com/articles/article.asp?p=1998559

Ross, R. S., & Swanson, M. M. (2004, February 1). Standards for security categorization of federal information and information systems. Retrieved November 21, 2016, from https://www.nist.gov/node/584996

Scarfone, K. A., & Mell, P. M. (2007). *SP 800–94. Guide to Intrusion Detection and Prevention Systems (IDPS)*. Gaithersburg, MD: National Institute of Standards & Technology.

Snyder, J. (2009). Do you need an IDS or IPS, or both? Retrieved January 12, 2017, from http://searchsecurity.techtarget.com/Do-you-need-an-IDS-or-IPS-or-both

STIGs Home. (n.d.). Retrieved January 2, 2017, from http://iase.disa.mil/stigs/Pages/index.aspx

Symantec. (2016). *Internet security threat report 2016*. Retrieved from https://www.symantec.com/security-center/threat-report

Tadda, G. P., & Salemo, J. S. (2010). *Overview of cyber situation awareness*. In S. Jajodia, P. Liu, V. Swarup, & C. Wang (Eds.) Cyber Situational Awareness (pp. 15–35). New York: Springer.

West, J., Dean, T., & Andrews, J. (2015). *Network + guide to networks* (7th edition). Boston, MA: Course Technology.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California