AN ARTIFICIAL NEURAL NETWORK-BASED DECISION-SUPPORT SYSTEM FOR INTEGRATED NETWORK SECURITY

THESIS
SEPTEMBER 2014

Tyrone A. L. Lewis Sr., Major, USA

AFIT-ENG-T-14-S-09

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-T-14-S-09

AN ARTIFICIAL NEURAL NETWORK-BASED DECISION-SUPPORT SYSTEM FOR INTEGRATED NETWORK SECURITY

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Cyber Operations

Tyrone A. L. Lewis Sr. BS

Major, USA

September 2014

AFIT-ENG-T-14-S-09

AN ARTIFICIAL NEURAL NETWORK-BASED DECISION-SUPPORT SYSTEM FOR INTEGRATED NETWORK SECURITY

Tyrone A. L. Lewis Sr. B.S.

Major, USA

Approved:

//signed//	August 26, 2014
Brian G. Woolley, Major, USAF (Chairman)	Date
//signed//	August 26, 2014
Kenneth Hopkinson, PhD (Member)	Date
//signed//	August 26, 2014
Michael Grimaila, PhD, CISM, CISSP (Member)	Date
//signed//	August 26, 2014
Timothy Lacey, PhD (Member)	Date

Abstract

As large-scale Cyber attacks become more sophisticated, local network defenders should employ *strength-in-numbers* to achieve mission success. Group collaboration reduces individual efforts to analyze and assess network traffic. Network defenders must evolve from an isolated defense in sector policy and move toward a collaborative *strength-in-numbers* defense policy that rethinks traditional network boundaries. Such a policy incorporates a network watch approach to global threat defense, where local defenders share the occurrence of local threats in real-time across network security boundaries, increases Cyber Situation Awareness (CSA) and provides localized decision-support. A single layer feed forward artificial neural network (ANN) is employed as a global threat event recommender system (GTERS) that learns expert-based threat mitigation decisions. The system combines the occurrence of local threat events into a unified global event situation, forming a global policy that allows the flexibility of various local policy interpretations of the global event. Such flexibility enables a Linux based network defender to ignore windows-specific threats while focusing on Linux threats in real-time. In this thesis, the GTERS is shown to effectively encode an arbitrary policy with 99.7% accuracy based on five threat-severity levels and achieves a generalization accuracy of 96.35% using four distinct participants and 9-fold cross-validation.

Acknowledgments

To my beautiful wife and best friend, thanks for your attentive ear and loving support. For my advisor MAJ Brian G. Woolley, and fellow committee members, I humbly express my sincere appreciation for your guidance and support throughout the course of this research effort. I dedicate this effort to better understand those who work tirelessly to defend our network boundaries against sophisticated global threats. Keep up the fight!

Thank you for this opportunity,

Tyrone A. L. Lewis Sr.

Table of Contents

Page

Abstract v
Acknowledgments vi
Table of Contents vii
List of Figures x
List of Tables xii
List of Acronyms xiii
I. Introduction 1
1.1 Problem Statement 10
1.2 Motivation 10
1.3 Hypothesis 12
1.4 Objectives 14
II. Literature Review 15
2.1 Situation Awareness 15
2.2 Team Situation Awareness Considerations 19
2.3 Historical Overview of Automation for the Intrusion Detection Process 20
2.3.1 Intrusion Detection and Prevention Fundamentals 22
2.3.2 Current Intrusion Detection and Prevention Systems Usage 24
2.3.2.1 Intrusion Detection and Prevention System Types 26
2.3.2.2 Multi-Level Architecture for Intrusion Detection and Prevention 28
2.3.2.3 Intrusion Detection Process as a Complex Adaptive System 30
2.4 Introduction to Emergence 31
2.4.1 Emergence in Communications Networks 32
2.4.2 Emergence as a Result of Local Policy and Objectives 33

2.5 Artificial Neural Networks 34
2.5.1 Fundamentals of Neural Network Engineering 35
2.5.2 Single Layer Feed Forward Artificial Neural Network Structure 36
2.5.3 Back propagation Gradient Descent Algorithm 38
2.5.6 K-Fold Cross-Validation 42
2.7 Chapter Summary 44
III. Methodology 45
3.1 General Problem Review 53
3.2 Problem Statement 57
3.3 Experimental Methodology 58
3.3.1 System Boundaries 59
3.3.2 Scope and Limitations 59
3.4 System Services 60
3.4.1 Decision Support Services 60
3.4.2 Off-Line Services 62
3.4.3 System Workload 66
3.5 System Performance Metrics 67
3.5.1 System Parameters 67
3.5.2 System Factors 70
3.5.3 System Evaluation Technique 72
3.5.4 Decision-Support Evaluation Technique 74
3.6 Experimental Design 74
3.6.1 Pilot Study Design (Scenario I) 74

3.6.2 Scenario II Single Decision-Support Profile Design 77

3.6.2.1 Scenario II Single Decision-Support Profile Baseline + Noise 80

3.6.2.2 Scenario II Single Decision-Support Profile Baseline+Noise+CV 80

3.6.3 Scenario III Group Decision-Support Profile Design 80

3.7 Methodology Summary 82

IV. Analysis and Results 83

4.1 Pilot Study Results 83

4.2 Scenario II- Analysis of the effects of Noise and Cross-Validation on Decision-Support Profiles 86

4.3 Scenario-III Multiple DSP Interactions Results and Interpretations 93

4.4 Scenario-III Group DSP Baseline+CV Results and interpretations 98

4.5 Chapter Summary 100

V. Conclusions and Recommendations 102

5.1 Significance and Contributions of Research 103

5.2 Recommendations for Action 104

5.3 Research Summary 105

Appendix A Decision-Support Profile Survey 108

Bibliography 151

Vita 155

List of Figures

Page

Figure 1. The General Situation, Isolated Security Boundaries in Cyberspace 3

Figure 2. Single Layer Artificial Neural Network adapted from (Heaton, 2012)..... 37

Figure 3. Target Learning and Stimuli Classification (Mitchell, 1997) 38

Figure 4. Conventional Threat Event Recommender System Scheme 46

Figure 5. ANN-Based Global Threat Event Recommender System 48

Figure 6. Lightning's Operational Block-Diagram..... 49

Figure 7. Local Decision-Support Profile Component under Test (CUT) 61

Figure 8. Lightning's Off-Line Training Parameters..... 63

Figure 9. Pilot Study Logical View of 4-Area IDPS Integrated ANN Structure..... 77

Figure 10. Logical ANN Scenario-II Performance ANN Structure 79

Figure 11. Logical Group Scenario-III ANN Structure 81

Figure 12. Pilot Study Results with Errors 84

Figure 13. Pilot Study Error-Free Dataset Results 85

Figure 14. Baseline Decision-Support Profile (Local Policy) 87

Figure 15. Single Decision-Support Profile Baseline +Noise Results..... 89

Figure 16. Single Decision-Support Profile Baseline +Noise+ CV Results..... 90

Figure 17. Single Decision-Support Profile Accuracy Summary Results 91

Figure 18. Single Decision-Support Profile Error Summary Results 91

Figure 19. Group Decision-Support Profile Baseline Results 95

Figure 20. Group Decision-Support Profile Baseline PPL Accuracy Results 97

Figure 21. Group Decision-Support Profile Baseline Error Summary Results 97

Figure 22. Group Decision-Support Profile Baseline+CV Results 99

Figure 23. Group Decision-Support Profile Baseline+CV Accuracy Results 99

Figure 24. Group Decision-Support Profile Baseline+CV Error Results 100

List of Tables

Page

Table 1. Intrusion Detection Types, Deployment and Scope (Scarfone & Mell, 2007).. 28

Table 2. IDPS Security Architecture Components (Scarfone & Mell, 2007)..... 29

Table 3. System Under Test Employing Back propagation (Mitchell, 1997) 36

Table 4. K-Fold Cross-Validation with Back propagation 44

Table 5. Protective Posture Level Operating Cost Adapted from (Defense, 2001)..... 51

Table 6. KDD99 Threat label Category Definitions (Hettich & Bay, 1999)..... 52

Table 7. Determining Local Decision Support Profiles (DSP) Strategies 62

Table 8. 10%KDD99 Threat Labels and Category Statistics (Hettich & Bay, 1999) 65

Table 9. Threat Risk Factor Mapping to Threat-Severity Level (Pipken, 2000)..... 66

Table 10. Pilot Study-1 Initial Global Policy Dataset w/Errors 75

Table 11. Corrected 32-Sample Dataset errors 84

Table 12. Individual's severity rating of KDD99 dataset's threat labels..... 125

List of Acronyms

ANN	Artificial neural network
CTSSB	Critical Task Site Selection Board
DoD	Department of Defense
DSP	Decision-Support Profile
DSS	Decision-Support System
GDTA	Goal-Directed Task Analysis
GTERS	Global Threat Event Recommender System
HB	Host Based IDPS
IDPS	Intrusion Detection and Preventions System
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
LAN	Local-Area Network
MODESTA	Modeling, Emulation, Simulation Tool for Analysis
NB	Network-Based IDPS
NBA	Network Based Analysis IDPS
NBA	Network Behavior Analysis IDPS
OSI	Open Systems Interconnections
PPL	Protective Posture Level
SA	Situation Awareness
SNMP	Simple Network Management Protocol
SUT	System Under Test (Lightning)
VLAN	Virtual Local-Area Network

WNB	Wireless Network-Based IDPS
XOR	Exclusive OR Function

AN ARTIFICIAL NEURAL NETWORK-BASED DECISION-SUPPORT SYSTEM FOR INTEGRATED NETWORK SECURITY

I. Introduction

Conventionally, isolating network security boundaries was an effective method of minimizing security vulnerabilities. Isolated defense worked well against targeted threats where the network security boundary was well defined. Today however, network security boundaries in Cyberspace span geospatial and geopolitical boundaries, making isolated network defense against globally occurring threats more undefined. To overcome this situation, this research calls for a strength-in-numbers approach to global threat network defense, where independent neighbors participate in global threat reporting. The hope is that the aggregated events can be filtered based on localized policy and interests to provide localized, customizable situational awareness and decision-support for isolated network defenders. Choosing the best course of action to implement such a collaborative effort can often be accomplished through modeling and simulation of the operational environment. The purpose of the modeling and simulation environment is to explore those conditions which likely provides the necessary information to support decision-making in real-time under similar conditions. This research effort develops such a simulated environment using a single layer feed forward artificial neural network (ANN) to provide the decision-support to the isolated network defender.

This chapter presents the background of the general problem and recent research efforts that are relevant to this research. After presenting the research problem statement formally, the motivation for conducting the research is discussed. The hypotheses of this research to include the objectives are laid out. Finally the chapter ends with a preview of the remaining chapters of this research.

We begin with a background of the general situation and larger problem of modeling and simulating large-scale communication networks. There are five distinct local area networks that are separated by a firewall in the large-scale network (Figure 1) that represents a subset of the larger Cyberspace (i.e. The Internet). Each LAN's local firewall provides specific filtering services for the LAN. Often times the configurations vary drastically, but as interests of the LANs become more similar, the configurations may also become more similar. The goal of the firewall, as a sensor, is to prevent unauthorized or undesirable traffic from entering the LAN security boundary. Sensors can take on several names in networking, to include access control lists, intrusion detection systems, intrusion prevention systems as examples. These sensors enhance the decision-maker's ability to monitor detect and respond to network security violations and threats. Appropriate responses enable the network security defender to win in Cyberspace. In static environments, where the threat is well defined, the strategic employment of sensors provides reliable decision-support. However, as the level of global threat sophistication increase, old rules may no longer apply for appropriate decision-making, and thus the strategy to win must be altered in a contested and dynamic operational environment of globally occurring threats.

The production of a plan or strategy to win becomes the courses of action that an entity hopes to attain as their winning goal, thus war-gaming is of significant importance for decision-makers, who desire to win. War-gaming is a conscious attempt to form a mental model of the area of operation's situation (Wade Norman, 2010). Conventional war-gaming methods employ the belt, avenue-in-depth and the box techniques to model and simulate the operational environment (U.S. Army, 2011). War-gaming is not strictly for the military, as business organizations employ terms like game-face, competitive advantage and corporate strategy.

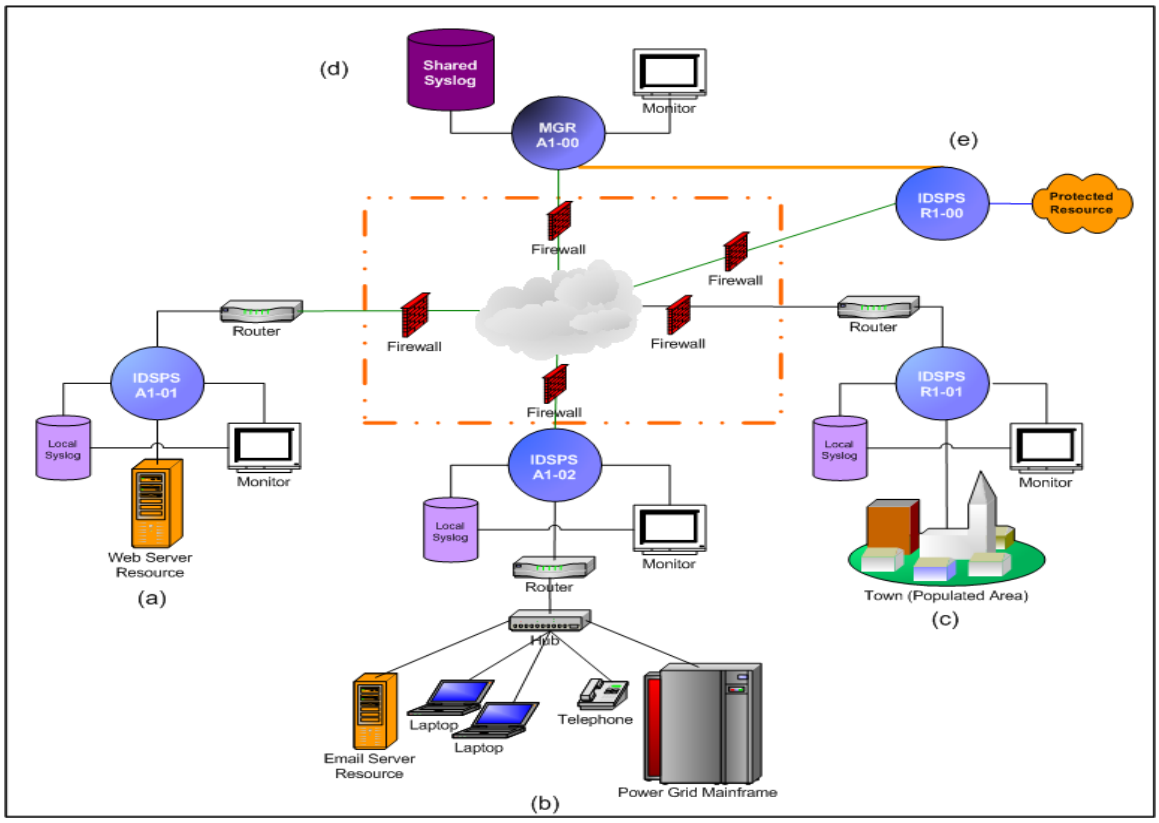

Figure 1. The General Situation, Isolated Security Boundaries in Cyberspace

For the business organization, war-gaming is the strategy, plans, goals and objectives that they hope to achieve in order to gain a competitive advantage and minimize costs against threat vulnerabilities or aggressive competitors. The strategy is often rehearsed, actions and reactions are simulated and courses of action are further refined and developed that yield the best courses of action. Each disparate LAN has an independent strategy to win according to their organizational goals and objectives. In (Figure 1a), a web server is being protected by the LAN's firewall and intrusion detection device. (Figure 1b) has a LAN that provides network security for a power grid, servers, telephones and laptop devices. (Figure 1c) shows a town as the protected network resource, while (Figure 1d) indicates an intrusion detection management LAN. Figure 1 depicts an intrusion detection device that provides service to an arbitrary resource.

Each LAN has a different set of protected resources, which needs a customized strategy to provide security vulnerability protection against a globally occurring threat event that crosses network security boundaries. These seemingly dissimilar LANs may share a common need to actively participate in defending against such a global threat. The development of a way to collaborate across network security boundaries would provide a strength-in numbers approach to defending against global threats, where the adversary's strategy is to win, by making organizations lose indiscriminately. Defining a mental model, which provides simulated globally occurring threat situations, may lead to a winning strategy in Cyberspace. Mental models are tools that help people think about how something works. Building and maintaining effective mental models where complex systems are involved; require significant data filtering, are dynamic in nature, are adaptive in nature and are can create significant challenges to obtaining good SA (Endsley & Bolte, 2003).

Modeling and simulating mental models that represent Cyberspace as an operational battlefield for good CSA, is an ongoing challenge for the Department of Defense (DoD). The National Cyber Range, using Strategic Initiative 2: *Employ new defense operating concepts to protect DoD networks and systems,* is intended to enable the military and others to address this need by simulating and testing new technologies and capabilities (U.S. Army, 2011). The Army is developing the Modeling, Emulation, Simulation Tool for Analysis (MODESTA), which is a holistic tactical modeling and simulations program that provides a large-scale systems–of-systems approach to modeling and simulating Cyber activities, which enhances decision-support and wargaming efforts in Cyberspace (Jontz, 2014). In fact, all branches of the US military are conducting research in Cyberspace and developing new ways to *operationalize* the manmade domain.

These efforts include the development of decision-support systems (DSS) and mental models that enhance the decision-making process by the Air Force's Research Laboratory (AFRL) and Air Force Institute of Technology (AFIT).

AFRL has declared Cyberspace as the *ultimate* complex and adaptive system, and acknowledges that the DoD must develop and integrate real-time situational awareness mechanisms to enable contextual understanding and enhance decision-making domains (Phister, 2010). Phister contends that the DoD will require more than just purely defensive measures to achieve information superiority in Cyberspace. He calls for required information technologies in the Cognitive, Social, Information, and Physical Domains in Cyberspace. This research effort hopes to make contributions in the cognitive, social and physical domains by developing a mental model of a simulated IDPS environment using an ANN-based recommender system.

The research models the LAN's culture to consist of the set of traffic-mix and the strategy to win given the traffic mix. The traffic mix is the traffic type (i.e. voice, video, data, Face book, email, secure voice, peak busy hour, bandwidth utilization etc.) that is unique to the LAN. No two sets separately managed LANs will have the exact same traffic mix. The organizational behavior modeling and simulation capability is derived from the local policy or threat mitigation responses that are appropriate for the organization that is providing network security defense. Information exploitation and understanding is achieved by providing the capability of localized interpretation of globally occurring events. These two items represent the cognitive and social domain elements of the research. The ANN-based recommender system represents the robust physical domain to provide real-time situation awareness and decision-support.

Mental models of simulated complex systems like intrusion detection and protection systems (IDPS) can provide information overload, out-of-the-loop syndrome and create complexity creep. As a result, full automation efforts can lead to inappropriate decision-making despite a change in the contextual environment (Endsley & Garland, 2000). The employment of the ANN-based mental model provides a partially automated solution that makes the best threat mitigation recommendation to the local network defender, given the occurrence of a global event.

Effective situation awareness in time sensitive environments is critical. In his thesis, Raulerson argued that cyber defenders must first have SA of their respective cyber networks in order to defend them (Raulerson, 2013). He went on to develop a tool that aggregates data from heterogeneous sensors creating a real-time network model using data fusion techniques for improved SA. Raulerson used the Common Vulnerability Scoring System to provide scores to vulnerabilities and attacks categories in the CVE online repository to conduct his risk assessment of protected resources (Raulerson, 2013). This research adapts the CVE and risk factor calculations methods provided by Pipken (2002). Finally, Raulerson's approach of aggregating from dissimilar sensors provided a SA picture using a centralized virtual machine to manage the network and demonstrated that data fusion using multiple disparate networks was beneficial.

This research differs from Raulerson's research effort in three primary ways. First, the ANN is employed as the communications infrastructure and the associated link weights are adjusted during training. As a result there is no need to maintain a central repository of threats. In Raulerson's the sensor's ability to identify malicious traffic directly from five different sensor devices and assesses the amount of information that an administrator utilizes as a measure of data reduction.

In this work, the second primary difference, the performance of the sensor devices are not considered in the evaluation of the SUT, instead the ability to recommend the protective posture level that matches expert human opinion is assessed.

Data reduction processing is not necessary for the network defender in real-time since the network's physical structure contains the weights that specify the level of information contribution from data resources (i.e. participant reports) this is significantly different from Raulerson's work because it directly introduces the human-element into the overall threat mitigation and avoidance control loop. By doing this, the SUT can interpret multiple sensor inputs and provide a locally defined threat-severity level that maps to a desired protective posture level to mitigate or avoid threats.

Each locally defined threat-severity level can then be mapped to a localized protective posture level. In the event that the pattern is detected in real-time, the ANN provides the protective posture level recommendation specified in the Decision-support profile. The decision-support profile is determined off-line and learned by the ANN during training. Finally, the third distinction from Raulerson's work, the resulting recommendation is customized for each independent participant based on their desired response given the global event detected using the ANN-based model. This capability provides a predictive decision-support capability for threat mitigation and avoidance. Because the ANN learns the expert's desired-response, the local network defender does not have to process the details of the recommendation in real-time event detection. In Raulerson's work, there is no method to provide customized real-time decision-support without the administrator's assessment afterwards.

In research by Lyons (2014), a predictive recommender system that provides the Cyber defender a list of recommended defense actions based on information gained from nearest neighbor similarity assessments. Prior to this, little research had been conducted to develop a pure recommender system for cyber defense (Lyons, 2014). Although the research did not provide significant insight into comparable predictors, additional effort in this area may yield benefits.

From such inspiration, this research integrates IDPS agents from separate large-scale dissimilar networking environments using a single feed forward artificial neural network to generate security posture recommendations. Such recommendations are based on an aggregated global policy that provides localized recommendations for decision-support, which is different than presenting the network defender with a list of options as the decision-support mechanism. Furthermore, this method does not store reports in a central repository, instead the ANN structure provides a link-weighted structure that aggregates the contribution level of reports from several IDPS sensors and learns the appropriate response.

An ANN's structure is a subset of complex adaptive system (CAS). The definition for a CAS in this research is: A complex system containing adaptive agents, networked so that the environment of each adaptive agent includes other agents in the system (Holland & Miller, 1991). The IDPS agents utilize three simple rules of monitoring their operational environment for unwanted traffic, detecting the status of unwanted traffic behavior and reporting the status of critical SA element cues to decision-makers. Because the global Internet or Cyberspace in this context is comprised, of dissimilar and independent local area networks (LANs) they are represented as IDPS agents who provide IDPS services in the intrusion detection and prevention process (IDP). The emergent behavior of their independent threat reporting is learned by the ANN and recommends a threat mitigation protective posture level (PPL) to local decision-makers.

This thesis abstracts the IDP as a working model to investigate a specific case of how critical cue elements influence the war fighter's SA and decision-making in collaborative environments. For example, the research shows that when sharing threat information, a decision-maker is presented with a clearer picture of globally occurring threats not only for their local environment, but also for threats occurring at participating neighbor networks. As a result, this additional threat awareness provided by neighbors may provide actionable information to local-decision-makers if the neighbor reports are interpreted as something meaningful to the local area. Neighbor reports enable local decision-makers to make informed decisions on how to mitigate and avoid threats against their local network boundary, thus the reports provide local decision-support. Collaborative teams working toward a common goal of threat mitigation, has strength-in-numbers for network defense by sharing neighbor reports. By incorporating collaborative threat mitigation across security boundaries, interested business organizations and the DoD may benefit from collaborative neighbor reporting in Cyberspace.

The experimental results of the DSS show a 99.7% recommendation accuracy when trained exhaustively over small situation sets and a generalization accuracy of 96.35% (i.e. 9-fold cross-validation) when recommending protective postures for previously unseen threats. The research shows how an individual's independent report of locally occurring threats contributes to a global threat operational picture and thus an increased situational awareness for the isolated network security boundary defender in Cyberspace.

Having provided an overview of the general problem, the research problem is presented in the next section. The aim of the problem statement is to focus on the Cyberspace security professional's task of defending their network security boundary in a large-scale intrusion detection and prevention environment.

1.1 Problem Statement

How can disparate expert security professionals share information across virtual network security boundaries while providing localized decision-support to novice defenders? The problem should be addressed because the research effort enables novice local network defenders to make more appropriate and informed threat mitigation decisions. Often times, cultural or local policy prevent the sharing of threat information, leaving an isolated network defender vulnerable despite the existence of a true global threat that crosses network security boundaries in Cyberspace. If reports of the occurrence of threats are received in a timely manner to novice defenders, situation awareness may provide actionable decision-support in the defense of protected resources. The desire to assist the isolated defender leads to the motivation of this research.

1.2 Motivation

The motivation of this work is to assist the novice local network defender who has the complex task of network security and defense. Such novice defenders tend to rely solely on their intrusion detection and prevention systems to assist their decision-making, best practices and their own local policy guidance to achieve their organizational goals and objectives and less on higher levels of situational awareness.

How will our defenders act in isolation when unaware of globally trending threats which their networks are vulnerable? Physical isolation is a conventional method of minimizing vulnerabilities in a world where security boundaries are more defined (Ware, 1970). In Cyberspace, these previously defined physical network security boundaries become only virtual or semantic for a global adversary. The thought that isolation of a network provides the best defense strategy in the face of a globally occurring threat is just as conventional and outdated.

An isolated or unaware network defender is placed at a disadvantage against globally occurring threats. Employing group participation (i.e. strength-in-numbers) provides a method to minimize risk against globally occurring threats that cross network security boundaries. Such a method provides a greater benefit to defend against blind spots for network security. Previous leakage (Ware, 1970) of security vulnerabilities becomes a *blind spot* in Cyberspace in some situations like the mega breeches mentioned in a recent report, where personally identifiable information was compromised from public information systems (Symantec, 2014). This research effort hopes to contribute to the cause of providing collaborative network defense strength-in-numbers for those network defenders that desire to minimize risk against global adversaries that disregard conventional network security boundaries.

As other nations develop controls within Cyberspace as weapons, so too must the United States, which remains vulnerable by the very manipulation of information that could put the nation at a significant disadvantage and cripple our protected resources such as industrial control systems. By studying the nature of CAS, trust convergence, and the emergent behavior of globally occurring threats in intrusion detection and prevention networks, this research adapts the concepts found in conventional neighborhood watch programs. Artificial Neural Networks (ANNs) concepts are employed to offer a neighborhood watch like protocol for global threat mitigation and avoidance. The resulting emergent behavior of real-time threat event collaboration between groups of participating *neighbors* may provide actionable recommendations and decision-support for local decision-makers.

1.3 Hypothesis

Effective Cyber SA can be achieved by employing an artificial neural network as a global threat event recommender system (GTERS) in intrusion detection and prevention environments. ANNs can encode expert security professional's decision-support profiles for network intrusion detection and prevention networks to enable report collaboration across network security boundaries and make best-fit protective posture level recommendations in uncertain situations. The ability to collaborate across network boundaries provides a strength-in-numbers approach to defense that provides decision-support to novice defenders based on expert knowledge.

The research aims to demonstrate a DSS capable of encoding expert user's decisions about what threat protection posture level is most appropriate given a particular set of threat indicators. Such a system is intended to serve as a recommender system in the absence of an expert security professional.

To accomplish this, a single-layer feed-forward artificial neural network (ANN) customized with the back-propagation gradient descent algorithm to map the status of multiple local threat event detections as reported by IDPSs. The aggregated IDPS event reports are then used as stimulus to the ANN while the ANN response is used to recommend a best-fit protective posture level that matches the local-decision maker's desired response. The simulations environment provides a mental model to facilitate the development of the decision-support concept. The focus of this research is on the capability of the ANN to provide security posture level recommendations based on external network threats. The IDPSs are considered as being interconnected across a simulated secure communications infrastructure on a separate management network. Participants in the collaborative network are considered fully trusted.

The results of adjusting the learning rate of the ANN with 0.005, 0.3, 0.7 and 1.0 values show that the ANN can accurately recommend the learned protective posture levels of expert decision-makers 90% of the time using a noisy decision-support profile and 9-fold cross-validation. Without cross-validation or noise the ANN has a recommendation accuracy of 99.7% for the baseline profile. When tested using four independent decision-support profiles in collaboration, the ANN's average generalization accuracy improves to 96.35% without noisy decision-support profiles and 9-fold cross-validation. The research shows significant accuracy for group collaboration using ANNs.

Having the capability to enable the novice network defender's decision-making using expert decision-support profiles is a significant step towards global-threat defense in collaborative network security environments. The ANN's ability to encode independent threat reports into an aggregate global event provides the isolated defender with customized situation awareness about local threats of interest. Employing the generalization capability of the of the ANN structure to provide localized decision-support is different from any of the previous research efforts. The data implies that as more network defenders participate, a more representative global threat picture begins to emerge from the localized reporting actions of dissimilar defenders.

The ANN provides a robust and meaningful way to provide situational awareness about global threats that are occurring locally and those that are occurring against trusted neighbors. Such a capability can lead to effective strength-in-numbers, early warning capability, and reduce threat mitigation cost for Cyberspace security professionals. Having provided the specific research problem statement, hypothesis and motivation to conduct the research, the objectives are presented next.

1.4 Objectives

This research has three objectives. (1) Design, build and model a wide-area interconnected network using a software simulation package that will be used as the mental model to facilitate understanding and evaluate the testing of the experimental objective. (2) Determine the effects of the interactions of critical element cues needed for SA and network defense in Cyberspace. These critical element cues will be modeled in the simulation to represent the status of monitoring, detecting and responding to threat traffic. And (3) to determine the effects of employing an ANN, which encodes local expert decision-support profiles and recommends the best protective posture level given the occurrence of a global threat event in a simulated collaborative event detection environment.

The rest of this research is organized as follows; a literature review in Chapter II frames the situation of the intrusion detection process (IDP) that describes the behavioral interactions of the decision-maker and the intrusion detection and prevention system (IDPS) as the DSS. The system under test (SUT), research methodology, experimental hypothesis and the approach to achieve the experimental goals are found in Chapter III.

The experimental design was performed using a pilot study, single noisy decision-support profile scenario and a group collaboration scenario. The scenario results are then presented in chapter IV. The conclusions, contributions and future research recommendations are provided in Chapter V. The Appendix contains a survey to develop advanced decision-support profiles of Cyberspace security professionals.

II. Literature Review

"Behavior is a difficult subject matter, not because it is inaccessible, but because it is extremely complex. … It is changing, fluid, and evanescent, and … makes great technical demands upon the ingenuity and energy of the scientist" (Skinner, 2005).

To understand how Cyber SA can be enhanced by a decision-support system (DSS), a brief introduction of situation awareness and decision-making provides the necessary background on the development of intrusion detection and security automation. A brief historical overview of literature that explains the intrusion detection process (IDP), which describes a custom relationship that exists between a human and the DSS, is made. After intrusion detection and prevention fundamentals and their employment strategies have been explored, a review of the phenomenon called emergent behavior and complex adaptive systems are discussed.

2.1 Situation Awareness

Situation awareness (SA) is defined as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" (Endsley & Garland, 2000). Effective SA has three components. Perception of the elements (the basic cues to make a decision in a given situation or context) in the environment is the first component and provides Level-1 SA. Challenges for modeling and simulation arise when representing relevant elements that occur in an operational environment, as decision-support cues must be customized to support a specific, not generic, individual's mental model.

For the IDP, the element is the threat signature, label or perception of some unwanted or undesirable behavior that occurs or originates from external traffic mix sources. The traffic mix is the data that the IDPS filters for a network security boundary. The elements can change depending on the time of day, the interpretations of an element's status and meaning or several factors that may contribute to why an element is a cue.

The second component of SA is the comprehension of the current situation and represents Level-2 SA. Understanding and synthesizing the interactions of element cues are critical in providing decision-support that enables the successful attainment of organizational goals and objectives. Level-3 SA is the projection of future states and is the last component of SA. After perceiving the status of the elements (Level-1), synthesizing now they interact in a particular context (Level-2) the user is now able to predict the status of the elements in the near future (Endsley & Bolte, 2003). Projection can thus be formalized as understanding what the current situation means to you in the future. At the lowest level (i.e. survival) projection is the recognition of danger in a given situation. Such projections then shape decision-making.

As Cyberspace security professionals perform the IDP to protect their network boundaries, they employ DSSs to assist and shape their decision-making. In isolated network defense environments, the network defender's local DSS can only provide shaping support for locally occurring threats. The decision-maker must find alternative decision-support avenues to gain a global situational awareness (i.e. contact higher authorities to determine if some unknown traffic is malicious or not). By enabling collaboration of threat reports, perhaps the time to provide meaningful decision support could have been achieved near real time.

A meaningful DSS enables the mental model of the decision-maker and allows for higher levels of SA to be achieved (Endsley & Garland, 2000). The role of mental models is to compliment DSSs and is invaluable to achieving good SA (Endsley & Garland, 2000).

As previously mentioned a mental model is a method that people use to better understand something and are key enablers of comprehension and projection. Endsley and Garland (2000) assert that mental models are systematic in nature and contain both a semantic knowledge and system knowledge of how something works. Semantic knowledge is the logical meaning or interpretation of something, where system knowledge knows about the more tangible components of how and what something is. In physical environments, systems knowledge is more concrete, while semantic knowledge can vary significantly (e.g. language).

In addition, experience plays a significant role in SA when using mature and experienced mental models. Experience with mental models can create a level of positive automaticity, which can appear as automatic behavior responses (Endsley & Garland, 2000). Positive automaticity is learned or reinforcement from previous instances (i.e. experiences) of making appropriate decisions in similar situations for the decision-maker. As the decision is made more often without negative consequences, the decision-maker is relieved of dedicating significant amounts of thought before making the decision. As a result, experienced decision-makers may appear to be in an automatic state when making decisions because of the positively reinforced decisions, which Endsley and Garland (2000) call automatic behavior.

When mental models provide positive results, SA can benefit because it frees up mental effort and allows higher levels of achievement for more challenging tasks. (Endsley & Bolte, 2003).

Caution should be used when developing modeling and simulation tools that provide a stale or old status of elements in dynamic operational environments, where behaviors evolve over time and the status of a particular element's meaning has changed with relation to the perceived or actual impact on achieving organizational goals and objectives. Making automatic decision using inappropriate element status perception can be detrimental. Mental models can incorporate validity, similar to playing poker, or risk assessments before automatically deciding to act on sensitive or priority tasks. In time-sensitive environments, the automated approach might be the best choice in uncertain situations when using an errant mental model.

The ANN's ability to provide an approximated best-fit protective posture level based on the mental model of an expert security professional will be assessed to determine how well the ANN's recommendation accuracy is when faced with *unseen* data. This measure of performance provides the generalization accuracy of the ANN recommender system. High generalization accuracy further enables the decision-maker to make appropriate decisions and accomplish their organizational goals and objectives, thus providing enhanced SA.

Endsley and Garland (2000) introduce a concept called goal-directed task analysis (GDTA), which is a design approach that focuses on the basic goals of the operator, major decisions needed to accomplish the goals and the SA requirements for each decision. Another approach is to use the Delphi study method (Turof, 1975), or the Army's Critical Task and Site Analysis Board process (Army, 2004). Both processes conduct an analysis of a job or skill set population and each have several phases that include interviewing human subjects, assessing the current skills, abilities, and required knowledge to be successful decision-makers.

These design methods can enhance mental model and simulation capability by obtain validation of the basic goals, decision of monitoring, detection and responding to intrusions and the perception and comprehension elements. This work presents a survey based on the SA model introduced by Endsley and Garland (2000) that is designed to develop an expert mental model that can be used to train an automated system for security professionals. In particular, the system presented here specifically address intrusion detection and prevention related jobs. Such surveys can take up to a year or more to obtain validated data. The proposed survey for this research has been included in Appendix A.

As expert DSPs are developed, in theory, the ANN can learn and recommend more complex protective posture recommendations to novice Cyberspace security professionals. In this way, team collaboration supported by ANN structures is warranted for future research.

2.2 Team Situation Awareness Considerations

Endsley and Garland (2000) define team SA as "the degree to which every team member possesses the SA required for his or her responsibilities". Interestingly, team SA is different from SA in that it is the degree to which all members have the *same* SA on the *same* requirements.

Shared SA requirements should include shared SA devices, mechanisms, requirements and processes for those teams. These requirements can be determined using survey techniques like the Delphi Method, the CTSSB, or the GDTA job analysis surveys. These methods focus on the overlap of shared requirements. The realization here is that such concepts for SA are directly applicable to the defense of network security boundaries.

2.3 Historical Overview of Automation for the Intrusion Detection Process

Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible *incidents,* which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices (Scarfone & Mell, 2007). An *intrusion detection system* (IDS) is software that automates the intrusion detection process.

An *intrusion prevention system* (IPS) is software that has all the capabilities of an intrusion detection system and can attempt to stop possible incidents. Both devices are used interchangeably and will be referred to as Intrusion detection and prevention systems (IDPS).

Hart (2005) provided a history of intrusion detection systems, in which he identified three factors that contributed to the need for intrusion detection. The first is increased acquisition and usage of resource-sharing systems in the DoD. A growing need to employ resource-sharing systems within an open computing environment while maintaining security was the second factor. Resource-sharing systems are those that distribute the resources of a computer system, allowing geographically separated people the capability to work on the system concurrently (Ware, 1970). Ware (1970) further asserts that security boundaries vulnerabilities are leakage points that come in five groups: physical surroundings, hardware, software, communications links, and organizational (i.e. personnel and procedures). Employing a combination of protection features can safeguard the leakage points.

Interestingly, Ware (1970) called for an immediate modification to policy to allow military centers and contractors to acquire and operate such systems. This call led to the development of security audits on these geographically separated *resource-sharing* systems and the third factor in the development of intrusion detection.

The third factor that led to the creation of intrusion detection, *Unmanageable volume of audit data being produced*, contributes to the motivations of conducting this research effort (Hart, 2005). Intrusion detection emerged as a discipline from computer security where the focus is on *resource –sharing* systems.

A standard vocabulary for discussing intrusion detection was provided by (Anderson, 1980), which and outlined the fundamental problem of conducting a security audit trail. Anderson argued the following: that independent audit trails from multiple systems are more difficult for security analysts in networked environments to analyze in real time.

Instead, Anderson proposed a *security monitoring surveillance system* that would automate the process of conducting security audits. Furthermore, he suggests that a correlation of events between groups would provide additional granularity for identifying abnormal behavior. Providing information in real-time was an enduring challenge. Analysis of the first intrusion detection models revealed that IDPS initially fell into two distinct categories: *anomaly detection* and *signature detection* (Denning, 1986).

The next milestone for IDPS occurred with the introduction of the Network System Monitor (NSM), which provided the ability to monitor network traffic (Bace, 2000). The Distributed Intrusion Detection System (DIDS) was the first integration of host and network-based intrusion detection capabilities and garnered large-scale support from the U.S. Air Force, the National Security Agency, and the U.S. Department of Energy (Hart, 2005). The DIDS established itself as the first integrated tool for collecting and correlating evidentiary data related to computer misuse, which is a key feature of today's forensics tools to support computer crime investigations.

This section provided the historical creation of the intrusion detection system that formed the anomaly detection and the signature based detection initial categories. The next section describes two additional IDSP categories, the fundamental functionality of IDPS, their types and typical operational employment.

2.3.1 Intrusion Detection and Prevention Fundamentals

A network security boundary experiences the arrival and departure of networking traffic in ways that match the organizational culture, design, communications needs and network services. Collectively, the characteristic of the network traffic that enters and departs a network security boundary is considered its traffic mix (e.g. a voice network may have a high traffic volume of voice data using UDP, but only has low TCP traffic for file transfers.

The ability to *monitor* a given traffic mixture within a specific computing area, *detect* suspicious, malicious or unwanted traffic signal activity, and *report* to those detected signals are inherent to all software or hardware based intrusion detection devices. Devices with additional proactive *response* abilities are called IPS, because they actively provide prevention and protection for selected critical-resources. This research combines such capabilities in a simulated environment to show how collaboration among distinct networks enhances the protection of critical-resources. The process of intrusion detection requires an evolving role-sharing partnership between a Cyber security professional's decision-making ability coupled with an IDPS ability to filter and classify traffic mix, detect undesirable traffic, and report intrusive (i.e. malicious) activity. Given the volume and rate of data entering such a network, the Cyber security professional's ability to make informed decisions on how to best protect network resources depends heavily on their ability to configure and interpret reports from the IDPS.

Such responses then can be translated into configurations for the IDPS. The goal is to allow the IDPS to handle threats based on the configurations rules so that the security professional can then make informed, appropriate and timely decisions.

Knowledge of network behavior and situational awareness are critical skills of a Cyber security professional. The Cyber security professional, in fact, it is the IDPS's ability to provide information summarization that creates enhanced situational awareness. This interdependency works well for Cyber security professional's that have a mature understanding of their managed networking environment and a deep understanding of the IDPS configuration rule-sets.

This relationship between the security professional and the IDPS is critical in that a weak point will increase the workload of the security professional. In this way, the security professional increases the workload of the Cyber security professional. In this regard, the Cyber security professional is performing the monitoring, detecting, and reporting of the network conditions rather than allowing the IDPS to be automated extension of their capabilities.

This conventional relationship creates two bottlenecks. One exists with the automation of the device itself. Although the device is capable of precisely processing and detecting signals near network speeds with an average delay of 1 microsecond, its accuracy becomes inappropriate in dynamic network environments (Carter, 2006). However, if no signature matches, then the nefarious traffic will go undetected by the IDPS.

Such an inability to adapt to the varying traffic signatures degrades the effectiveness of the IDPS, and places a larger load on the decision-making of the Cyber security professional. The other bottleneck is the security professional's lack of appropriate situational awareness, either within their local network or with dispersed networks within the same organization.

Such a lack of situational awareness leads to an incomplete understanding the operational environment and an inability to apply appropriate configurations that support their local network. Together, the Cyber security professional's decision process and the IDPS's detection ability, determine the accuracy and precision of the IDP.

The Cyber security professional is continuously monitoring their network conditions, enacting policy and operational changes. Cyber security professionals are interested in defending their assigned critical resources within their area of responsibility and monitor the response(s) of their IDPS for signs of intrusions, an alerting signal indicating a need to modify or repair their device(s), or a need to make decisions that will mitigate, shape or prevent future intrusions within their direct or supported networking environment.

2.3.2 Current Intrusion Detection and Prevention Systems Usage

Modern IDPS systems are primarily focused on identifying possible incidents. In particular, their primary role is to identify reconnaissance activity that could indicate imminent attack on protected internal networks (Scarfone & Mell, 2007). Due to an increasing dependence on IT and potential impact of an intrusion against those systems, IDPSs have become a necessary addition to the security infrastructure (Scarfone & Mell, 2007). Some critical aspects of intrusion detection devices include their type, functions, major capabilities, implementation strategies, and interconnectedness.

Key functions of all intrusion detection and prevention devices are monitoring, detecting and reporting events. Reporting and alert methods are conventionally done in the form of email, IDPS GUI, syslog messages, SNMP traps, custom defined scripts(Scarfone & Mell, 2007).

A report provides detailed information about the conditions of the network during the occurrence of the alerting event. More advanced devices are capable of preventing intrusions in addition to simple detection capability.

Prevention functions include automatic modification of user security profiles when a new threat is detected and are designed to prevent three categories of attacks (Scarfone & Mell, 2007). Category 1 includes stopping the attack by terminating connections or settings, blocking access to target devices from the offending source, and blocking all access to the target from the offending source. Category 2 includes changing the security environment by modifying the configurations and settings of other security controls to disrupt an attack. Reconfiguring router access control lists, altering host-based firewall settings, and applying patches to a host if the IPS detects host vulnerabilities are examples. Category 3 changes the content of the attack payload, removes or replaces malicious portions of an attack's payload to diffuse potentially destructive capability. This is accomplished by file removal of suspicious emails or by packet-normalization where a packet is inspected, and repackaged after suspicious content has been discarded.

Despite such abilities to prevent these three categories of attacks, malicious or unintentional security violations can still occur through user evasion, dynamic malware payload, or simple modifications to existing exploitation techniques. To defend against this, a tuning process must be continuously conducted between the device and the Cyber security professional to achieve maximum performance levels. The tuning process can be formalized for intrusion detection and prevention methods to protect against these categories of attacks.

There are four primary detection methods used by today's IDPS. The first method is called Signature-based. The signature-based or *misuse* detection method detects patterns that correspond to a known threat.

This is the simplest form of detection, but a Cyber security professional's lack of understanding of *misuse* is confounded with multiple user application usage. Anomaly based detection (ABD) is the second detection method. This process monitors and compares observed events to normal baseline traffic behavior. This is an effective technique but is resource intensive to construct a common operation picture that describes normal behavior of the network and individual user profile patterns. The third method is called State Protocol Analysis.

The process of state protocol analysis is an advanced version of the signature-based process where collective trusts of signature definitions based on protocol usage are shared. Comparisons of these predetermined signature profiles are made against observed events to identify any deviations. Trust dominates this concept because a vendor specific profile specifies how a protocol should or should not be used (Carter, 2006). Finally, the last primary method of detection is the Combination. The combination method provides a mixture of the above methods. Using multiple methods of detection enables the security professional the opportunities reduces the overall security risk and reduce leakage that may arise from just a single method alone. This method is usually more costly and complex to maintain however provides more accurate and broad coverage of the protected network resources. Raulerson's research employed multiple sensor types in his research, which was found to be beneficial (Raulerson, 2013).

2.3.2.1 Intrusion Detection and Prevention System Types

There are four types of intrusion detection devices (Scarfone & Mell, 2007). Each type has a recommended monitoring scope and likely places that the device can be employed in the network boundary to detect transport or layer three and four protocol of the open systems interconnections (OSI) model.

The network behavior analysis (NBA) type of IDSP is typically used to detect traffic mix violations that would cause denial of service to the organization's network services or resources. NBA systems are found inside network boundaries to detect insider threats, outside network boundaries to detect outside threats, and between the two dispersed, yet commonly managed network boundaries when an organization is geographically dispersed.

The network based (NB) IDPS is typically employed to monitor network segments and analyzes segments of the network for suspicious traffic at the application layer of the OSI model. NB IDPSs can be found placed between separately managed network security boundaries and close to mission critical resources.

Wireless network behavior (WNB) IDPS are customized to detect malicious traffic like the NBA and NB types, however the NB has specialized ability to detect the wireless medium transport protocols (i.e. Wi-Fi, hotspots). WNB can be found near an organization's primary point of presence that provides wireless networking services to customers. The actual device is employed in a location to provide the best detection of malicious traffic to protect authorized wireless customers within the wireless security boundary.

The host based (HB) IDPS is the oldest type and is typically employed to provide IDP for a specific network device or individual host. These types can be found near mission critical resources within network security boundaries, i.e. secure data storage areas, financial web servers, industrial control devices, databases that contain personally identifiable information, (Scarfone & Mell, 2007).

These IDPS types are summarized in Table 1 and can be employed to meet the needs of the security professional, and usually are managed using from the same network that the device filters traffic on. A multi-level architecture involves the management of IDPS devices that provided filtering services on more than one network interface card and in multiple IP address spaces. Multi-level architectures are discussed next.

Table 1. Intrusion Detection Types, Deployment and Scope (Scarfone & Mell, 2007).

Type	Monitoring Scope	Deployment
Network Behavior Analysis (NBA)	Unusual trafic Flows like DDoS, worms,. Policy violations.	Inside ORG boundaries to monitor flows. Outside ORG and between ORG boundaries
Network Based (NB)	Network Segments. Analyzes for suspicious activity of network application protocols	Between Seperately Managed Network Boundaries. Close to other security devices.
Wireless (WNB)	Wireless network traffic and analysis of the protocol itself.	Near ORG Wireless Points of Prescense or areas were unauthorized wireless activity is suspected
Host (HB)	charasteristics of the single host only.	Critical Host Systems. Sensitive Information. Publicaly Accesible Servers

2.3.2.2 Multi-Level Architecture for Intrusion Detection and Prevention

To avoid attacks on the security system itself, the management network is hidden from other network traffic using a separate physical network interface (Scarfone & Mell, 2007). In this way, one network interface is used in the filtering of a network's traffic mix (inbound or outbound), while the other is reserved for the secure management of the IDPS system. There are three benefits to having a hidden management network: 1) bandwidth assurance, 2) concealment of IDPS identity from malicious users, 3) and protection from attacks.

Some disadvantages to maintaining a separate management network include additional cost to maintain the network, which is easily mitigated with the implementation of virtual local area network (VLAN). The major components of the IDPS architecture will be discussed next.

There are five primary components in the IDPS security architecture. The primary IDPS is often called sensor components because it provides the monitoring, detection and reporting of configured signatures. Sensors are used for all four types of IDSPs. The second components are agents, which are typically deployed in host-based IDS employment configurations. The management server component provides a way to centralize and correlate information from multiple IDSP that are dispersed through a commonly managed network security boundary. The database server component of the security architecture provides a repository for event information storage of IDPS reports that agent components and sensors provide to the management server. The last component, console, is the component that provides a visualization of the intrusion detection process for the security professional. IDPS. Table 2 provides a summary of the IDPS security architecture components found in the special publication of the National Institute of Standards and Technology 800-94. (Scarfone & Mell, 2007).

Table 2. IDPS Security Architecture Components (Scarfone & Mell, 2007)

Component	Monitoring Description
Sensor	IDPS that monitors networks (NBA, NB, WN and HB)
Agent	Conventially used for Host-based
Management Server	Centralized device that Correlates information from Agents and Sensors
Database Server	Repository for event information storage of reports received from Agents and Sensors.
Console	Management GUI for the system analyst

Having discussed IDP and IDPS fundamentals, the concept of what an agent is can now be introduced for this research. The IDPS represents the decision-support agent that uses the three IDP rules of monitoring, detecting and reporting of malicious traffic. The agents provide network boundary protection for the entire local area of interest in the modeled IDP environment. In this way, the IDPS agent is a HB that has sensor capability for the entire LAN. Due to the nature of the IDPS as an agent, we discuss the role of the agent in complex adaptive systems during the next section.

2.3.2.3 Intrusion Detection Process as a Complex Adaptive System

Holland and Miller (1991) introduced the concept of complex adaptive systems (CAS). This work describes a system that consists of a network of interacting *agents* that exhibit a dynamic, aggregate behavior. The behavior emerges from the individual activities of the agents and as a result, its aggregate behavior can be described without a detailed knowledge of the behavior of the individual agents. This ability to define an observable behavior or response without understanding the underlying conditions that brought about the condition is the discovery of emergent behavior phenomenon. Holland and Miller (1991) also define a complex adaptive agent (CAA) as an agent that satisfies an additional property of possessing the capability within a CAS to be assigned a value and the agent behaves to increase this value over time, thus forming the basis of a learning system. The definition for a CAS in this research is: A complex system containing adaptive agents, networked so that the environment of each adaptive agent includes other agents in the system (Holland & Miller, 1991). Phister (2010) refers to Cyberspace as the Ultimate CAS and outlines the challenges faced by the DoD to model and simulate a Cyberspace battlefield for military support operations (Phister, 2010).

This research models a large-scale IDP simulation environment as an interconnected set of IDPS, acting as complex adaptive agents. The independent actions of each IDPS agent provide threat reports that are occurring at their local network security boundary. The ANN's CAS structure is employed as the primary enabler of the aggregation of the independent agent reports. The result of these aggregated reports realized by the ANN structure provides protective posture level recommendations in real-time as decision-support for the Cyberspace network security professional.

Section 2.3 discussed current usage of IDPS as DSS, their functions, types, and architecture and how this research simulates a networked environment using sensory IDPS as agents to form a CAS. The phenomenon of emergent behavior discovery is a goal of this research and is introduced next.

2.4 Introduction to Emergence

Agents performing three simple rules create a situation where the development of a mental model, which explains a larger behavior, seemingly disjointed and very complicated. How can the aggregate reporting of independent agent components of network security boundaries somehow yield an emergent behavior that provides enhanced SA to network security professional? In his seminal work, Lewes (1875) asserts, "Every resultant is either a sum or a difference of the co-operant forces; … The emergent is unlike its components insofar as these are incommensurable, and it cannot be reduced to their sum or their difference" (Lewes, 1875).

Since, multiple disciplines have interpreted *emergent* to fit their particular needs Emergent behavior is most easily observed in naturally occurring systems like: riots, standing ovations, birds flocking in V-formations, bees swarming to maintain an average hive temperature, and ant colonization (Miller & Page, 2007).

Such naturally occurring behaviors are biologically based and variations occur in human society (Easley & Kleinberg, 2010). In the field of complexity, local emergence is where collective behavior appears in a small part of a system and global emergence occurs where collective behavior pertains to the system as a whole (Bar-Yam, 1997). Miller and Page 2007 argued that the Law of large numbers including the Central Limit Theorem can provide a theorem which explains the relatively general conditions under which certain types of emergent behavior from stochastic micro level levels actions of individual agents can arise. The Law of large numbers is one of several theorems expressing the idea that as the number of trials of a random process increases; the difference between the expected and actual values goes to zero (Renze & Weisstein, 2014). Thus the aim of this research is to study *how* the phenomenon of emergence occurs within a system of collaborating IDPSs that is interconnected using a single layer feed forward ANN. Adapting the universal nature of emergence, manmade controls to control emergence in communication networks are found in the next section.

2.4.1 Emergence in Communications Networks

Since all biological systems are results of evolutionary processes that show, robustness and adaptive powers (Floreano & Mattiusi, 2008), other disciplines develop algorithms that mimic the natural evolutionary process. Evolution in biology discipline is defined as: the change in genetic composition of a population over successive generations, which may be caused by natural selection, inbreeding, hybridization, or mutation, a concept introduced by Charles Darwin in 1809 (Quammen, 2008). Within the field of CAS, emergent behavior can occur as: *open-loop* emergent behavior or *feed-back loop* emergent behavior.

Open-loop emergent behavior is observed as a restructuring of a network from repeated applications of internal stimulus. A network's behavior that is restructured by external stimulus defines the process of *feedback-loop emergent behavior* (Lewis, 2009). In this research, local policies, organizational goals and objectives are the primary stimulus that contributes to open-loop emergence if it occurs. The traffic mix and any malicious activity detected represent the feedback-loop emergent behavior if it exists in this research. It is interesting to think about local policy as a contributing stimulus for open-loop emergent behavior and is discussed further in the next section.

2.4.2 Emergence as a Result of Local Policy and Objectives

Constraints are based on organizational goals, and are tested in this research only to observe the system for open-loop or feedback-loop emergent behavior characteristics, if it exists. Such constraints in learning systems may provide a good representation for local policy network defense. Local policy actions typically, only have local change of a larger governing system and occur at the tactical or micro level. It is interesting to see multiple individual local policies behaving together in sufficient numbers, that their collective behavior is seen as an emergent behavior, specifically open-loop emergent behavior, i.e. one that did not exist before and could not be expressed by an individual.

The process of developing the modeling a simulations environment enabled an intuitive understanding of how the application of the ANN as a CAS is able to aggregate the individual IDPS reports, and reveal the underlying mechanisms that generate the emergent behavior. The IDPS independently provide IDP services for their LAN. These individual actions can be characterized as independent variables for each LAN. Now we can assume that the LANs are mutually independent.

If the two LANs share a common distribution of network threats, have similar traffic mixtures, and similar local policy strategies for network defense, then one can assign an arbitrary value to their particular approach to network defense. The probability that the average or mean μ desired-response and situation events pairs differ (i.e. independent expert DSPs) by less than some arbitrary value tends to approach 1 as we increase the number (i.e. IDPS agents) in the collaborative system. In such a system, a stable aggregate property (i.e. Global Policy of learned DSPs), emerges from combining the reporting activities of the IDPS agents.

As discussed in Miller and Page (2007) the restriction is that the common distribution has mean μ, here the IDPSs average defense strategy is similar. This is profound for network defense and implies that the more similar in nature that LANs are, the more likely that their responses will be similar when faced with network threats. This research employs artificial neural network concepts to facilitate such network policies and to determine if this possible emergent behavioral response is significant.

2.5 Artificial Neural Networks

Artificial neural networks (ANN) are biologically inspired computational networks. The hope is that such a system may enhance the IDPS and security professional's decision-making cycle by acting as a DSS. This section discusses the fundamentals of neural network engineering that began as threshold logic, fundamentals of ANNs, feed forward single layer ANN structure, the back propagation gradient descent algorithm the sigmoid activation function and k-fold cross-validation.

2.5.1 Fundamentals of Neural Network Engineering

McCulloch (1943) established the term threshold logic that would branch into computational logic and artificial intelligence. Rosenblatt (1953) introduced the perceptron as a pattern recognition system based on a two-layer learning model. The perceptron's inability to solve the exclusive or (XOR) problem limited the pattern recognition systems to only linearly separable types of patterns (Floreano & Mattiusi, 2008). The implication is that the pattern could be divided into two groups, if a pattern was introduced to the system that did not distinctly fall into one of the groups, it could not be classified. Solving the XOR problem with additional computational units (i.e. hidden nodes) was accomplished using back propagation (Williams, Rumelhart, & McClelland, 1986) leading the way for additional gains in machine learning and artificial intelligence. Artificial networks are computational models of biological neural network systems in the form of software and hardware (Floreano & Mattiusi, 2008). In machine learning, artificial neural networks (ANNs) have the independent goal of obtaining highly efficient learning algorithms, despite the emulation of biological processes.

ANNs can provide practical methods of machine learning using algorithms such as back propagation and are the best among interpreting complex sensory data (Mitchell, 1997). The SUT code snippet employing the back propagation algorithm adapted from Mitchell (1997) and Wilensky (2006) is presented next.

Table 3. System Under Test Employing Back propagation (Mitchell, 1997)

Off-Line SUT Training with Back propagation Input to SUT

1. Initialize the network
   a. Create the Single-Layer ANN structure of inputs and output units.
   b. Select Threat-Severity Training Dataset$_i$
   c. Select Validation method: Training Dataset or K-Fold Cross-Validation
   d. Set Learning Rate: 0.005, 0.3, 0.7 or 1.0
   e. Set number of times each example is seen per at each training period : 1 (Epoch)
   f. Randomize link weights. (Usually close to the default threshold value of .05 and -.05)
   g. Establish running time termination conditions: 10
2. Until the termination condition is met
   a. For each occurrence of a value input and target concept, output pair (x_i, t_i) in the set of all training examples.
   b. Forward Propagate the input value x_i input values, link weight compute the observed output o_k
   c. Backwards propagate the errors:
      For each output-node *k*,
      calculate δ_k using eq. *(6).*
3. Update the link weights w_{ki} using eq. *(3)*

2.5.2 Single Layer Feed Forward Artificial Neural Network Structure

The basic structure of a single layer ANN has a number of input nodes. The input nodes provide the stimulus values that are passed forward through the network across the links which provide the ANN structure. Each link may contain a weighted value to provide the overall contribution of its associated input value. The summation of the input value multiplied by the link weight for each input is fed forward to the output node. The output node performs a learned target function on the stimuli and outputs a response value. (Figure 2) shows the basic schematic for a feed forward neural network model.

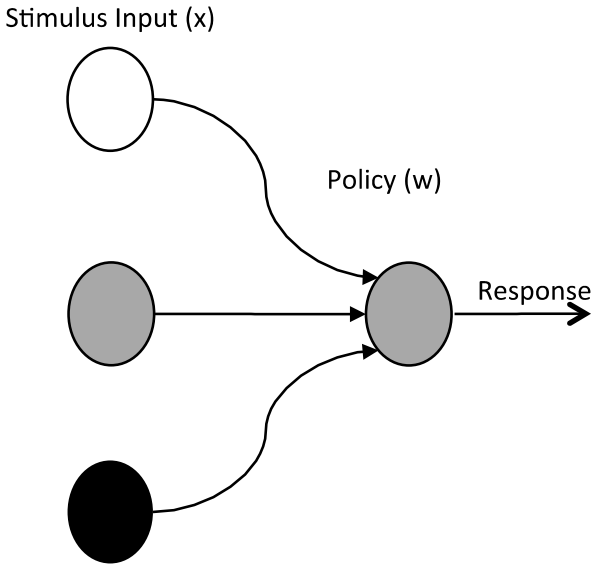

Figure 2. Single Layer Artificial Neural Network adapted from (Heaton, 2012)

In machine learning, these basic components are arranged as instances (input nodes), weight contributions (links) and learning function (output nodes). The target function is the classified output of the packet as either green to indicate a desirable packet or red that indicates an undesirable packet. On the left, a communications packet arrives as a stimulus instance or sample (Figure 3).

The input node (sensory unit) performs a classification function on the packet. The result of the classification function is forwarded to the output node along with the product of its corresponding link contribution. The output node applies a policy of any constraints within the hypothesis space on the contributed input. Finally, the output node responds with a response of the target hypothesis.

For packets classified as normal, the output node may provide a positive value and a negative value for malicious or unwanted classified packets. The nature of the output values can be determined by transfer functions and activation functions. A transfer function is an intermediary function that is applied to the initial weighted inputs. The transfer function conditions the data before sending to the activation function. The activation function choice varies based on the design objectives. Back propagation, a key training algorithm for ANNs, is discussed next.

2.5.3 Back propagation Gradient Descent Algorithm

Back propagation is a training algorithm that searches through a hypothesis space using an error function to adjust the weights of the neural network. During training, input values are provided to the ANN along with the desired target function's response.

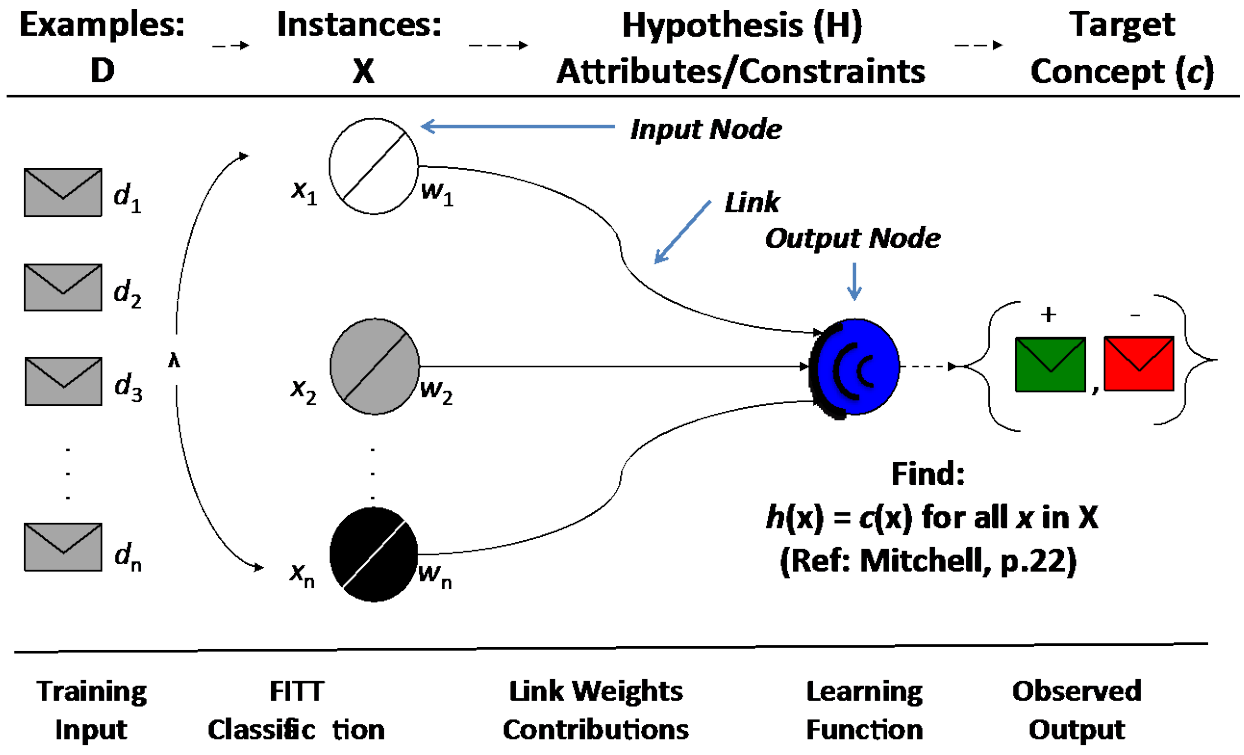

Figure 3. Target Learning and Stimuli Classification (Mitchell, 1997)

As each sample is presented to the ANN for learning, the actual response o_k is compared to the target concept $t_k$response. If the values do not match, then this is considering an error, *E* in the models' ability to learn the sample. To correct *E*, an error function takes the error and squares its value. This is called the means squared error (MSE). Back propagation then applies the error to adjust the link weight up or down in the direction that is needed to tune the link so that the same sample input and link value product provides a matching target and actual response.

As the weights are adjusted, back propagation updates the link values for the neural network structure (Heaton, 2012). The SUT employs a single layer feed forward ANN using back propagation, gradient descent function and the sigmoid activation function for the final performance test. The back propagation code for this research is adapted from the NetLogo modeling and simulations package (Wilensky U. , 2006). Gradient descent provides the basis for the back propagation function and converges to a minimum error weight vector set even if the samples are not linearly separable. Linearly separable data can be divided into distinct categories (Floreano & Mattiusi, 2008). ANNs that use threshold units can represent a rich variety of functions that the single perceptron unit alone cannot. The sigmoid activation function provides further representation of complex functions and pattern recognition producing a continuous function of its input (Mitchell, 1997). When training examples are presented to an ANN, using back propagation, gradient descent provides a way to tune the network parameters and approximate the closest matching set of input-output pairs.

The single layer feed forward ANN emergent behavior as a CAS employs back propagation and gradient descent to produce a vector of link weights that minimizes the error in the hypothesis space. The final link weights provide the ANN structure. When combined with the delta rule, gradient descent can be employed to enable stochastic approximation of nonlinear input-output pairs (Mitchell, 1997). If the learning rate is too large, the weight vector returned may only represent a local minimum error. When an error surface contains a single global minimum, but multiple local minimums, stopping in local minimum error zones can be reduced by using a lower learning rate (Mitchell, 1997). This learning rate parameter provides a partial method of controlling the ANN final link weight structure. After the link weights have been established to minimize the global error surface for the model, input values can be applied as a product of the link weight and transferred to an activation function, typically a sigmoid function (i.e. sigmoid). Each separate link and input value is forwarded through the network to represent the total stimuli that is presented to the activation function. The purpose of the activation function is to map the contribution of all incoming stimuli to the associated target concept.

Using gradient descent with the delta rule, weights are modified to reduce the error along the surface of the hypothesis space. The delta rule assists in overcoming the difficulty to reach a converged set of weights that minimize the hypothesis space. Using the delta rule along with gradient descent helps back propagation to minimize the hypothesis error surface and converge toward a best-fit approximation gradient specifies the direction that produces the steepest increase in E (Mitchell, 1997). Rumelhart's back propagation method is also known as the generalized delta rule, which can provide a solution for any ANN with an arbitrary number of neurons and connection layers (Floreano & Mattiusi, 2008). Lightning's back propagation code snippet is provided next before moving to k-fold cross validation.

The SUT code snippet is provided here;

```
to propagate
ask output-nodes [
   set activation new-activation
  ]
recolor
end

;; The backpropagation Algorithm for this Model

to back-propagate
  let example-error 0
   let answer desired-answer
    let s []

    ask A_Omega-node_Out_10 [
   set err activation * (1 - activation) * (answer_A10 - activation)
   set example-error_A10 example-error_A10 + ( (answer_A10 - activation) ^ 2 )
  ]

set epoch-error epoch-error + example-error
ask Avenues_Of_Trust [
   set influence-weight influence-weight + learning-rate * [err] of end2 * [activation] of
         end1

; Calculates the mean or average of all outputnodes MSE.  N = 20 HERE
set MSE ((
      epoch-error_A10 + epoch-error_A11 + epoch-error_A12 + epoch-error_A13 +
         epoch-error_A14
    + epoch-error_B10 + epoch-error_B11 + epoch-error_B12 + epoch-error_B13 +
         epoch-error_B14
    + epoch-error_C10 + epoch-error_C11 + epoch-error_C12 + epoch-error_C13 +
         epoch-error_C14
    + epoch-error_D10 + epoch-error_D11 + epoch-error_D12 + epoch-error_D13 +
         epoch-error_D14) / COUNT OUTPUT-NODES)
]
end
```

2.5.6 K-Fold Cross-Validation

It is desirable for a trained ANN to be able to classify data that it has never seen. If the ANN is trained to achieve 100% accuracy on the training data, the model tends to suffer when placed in an operation or online mode. This occurs because the weight vectors have been adjusted using gradient descent to minimize the error and move toward the global minimum. Although some cases may call for this type of behavior, complex adaptive system employments of sensory units call for the capability to generalize the training data. A model that performs poorly when faced with unseen data suffers from over fitting. Over fitting occurs when the model performs poorly against data that it has never seen although it performs well with the training data.

Generalization means that the weight vector set is sufficient to adequately represent the training data, but it can also approximate data that it has never seen before. Generalized behavior and accuracy is highly desirable in IDPS networks. Data Generalization and over fitting problems can often plague the reliability of the ANN when unseen data accuracy is sub-optimal. Generalization accuracy determines how well a model can accurately detect unseen samples. The generalization accuracy can be found by plotting the cross validation error against the training error. Cross validation is the process of training an ANN with the unhidden training data and then testing how well the model performed facing a hidden dataset.

At each interval of weight updates, the training error is validated against the hidden data. Since the validation contains data that the model has not seen, this is the best indicator of network performance over hidden samples (Mitchell, 1997). Running the process with multiple sets of link weights and selecting the best one can yield the lowest error over the validation set (Mitchell, 1997). This approach provides an additional set of data or hidden data as well as the original training data. When the training dataset is small, k-fold validation can be used.

Given a set of training situation events, randomly sort the training events. Next, separate the randomly sorted training events into k disjoint sets. each *k* size should be *m/k*, where *m* is the size of the total number of situation events in dataset *D*. After the training events are separated in *k* sets, take the last set and place aside. This set will be called the hidden fold dataset. Now, combine all remaining *k*-1 folds and separate (*k*-1) – 1 fold for testing during each validation round. While the folds remain untrained, partition the remaining modified folds and sort from lowest to highest and again, remove the last fold from the dataset. There are only seven folds that are presented to the ANN, and the eighth fold (last position) is used to validate those seven trained folds during that epoch. At the end of the training epoch and validation, add the 8^{th} fold back and shift all folds to the right so that fold eight is in position 0, fold one is in position one and fold seven is now the removed fold that is in position seven. Train, rotate and validate until all folds have been trained and validated. Once completed, validate the trained ANN model using the 9^{th} hidden fold. A summary of this process is provided in Table 4.

This section discussed emergence and its multiple meanings for several disciplines. It provided a working definition to describe emergent behavior in this research to be *open loop* or *feedback-loop* emergent behavior. The chapter summary is next.

Table 4. K-Fold Cross-Validation with Back propagation

K-fold Cross Validation with Back propagation:

Begin
1. Take Dataset D
2. Randomly sort D.
3. Partition D' into k disjoint sets each of size m/k
// Hide k-1 folds as the final testing set and is never trained.
set hidden fold (k-1)
4. Combine all remaining k-1 folds and separate (k-1) -1 fold to leave out for testing.
While folds remain to be tested
    Partition remaining D' into k' disjoint sets one size m/k and size (k-2)/k
    set m/k as testing_fold
    set (k-2)/k as training_fold
        Back propagate training_fold
        Validate training_fold with testing_fold
        //Update Errors
        Return Folds and Rotate
        Repeat all folds and rotation
10. Conduct Final Validation Test with Fold k-1 hidden.
Return Generalization Accuracy
End

2.7 Chapter Summary

This chapter presented a historical review of the need for intrusion detection and framed the automation optimization problem that exists between the security professional and the intrusion detection device. Having explored related works, concepts, theories and the simulation environment, Chapter III describes the methods and approach used to accomplish the research goal of identifying, characterizing, and describing *how the* emergent behavior of global threat collaboration and information sharing enhances local SA for decision-makers.

III. Methodology

"Nothing succeeds in war except in consequence of a well-prepared plan."

-Napoleon Bonaparte

This chapter provides the modeling and simulations approach used to define Lightning, the system under test (SUT) and conduct the performance evaluations. The general problem is summarized to transition to the research problem. Lightning is an ANN-based recommender system that differs from a conventional IDSP recommender system such that the ANN-based recommender system takes the conventional output of participating IDPS local threat event reports and combines the input into a global threat event. Based on the global event, the ANN-based recommender system provides customized local decision-support protective posture recommendations. Such a system is called a global threat event recommender system (GTERS) in this research. The left side of the conventional IDPS (Figure 4) indicates a level of preprocessing of the KDD99 dataset that a security professional must determine before making IDPS configurations and employing the DSS into the operational environment. After preprocessing, the IDPS can be employed in an operational environment to perform intrusion detection services according to the locally defined policy (i.e. configurations). An event is the occurrence of a known or unknown threat signature label that enters the network security boundary.

As local events occur the IDPS reports the status of the configured threat labels as events and may recommend a response to the local decision-maker or in some cases automate response actions. The detected label provides the stimulus for response action for the decision-maker in the conventional model of IDPS employment.

The GTERS model (Figure 5) extends the conventional performance of the IDPS fundamentals in a way that incorporates multiple DSS sensor reports combined into one event situation.

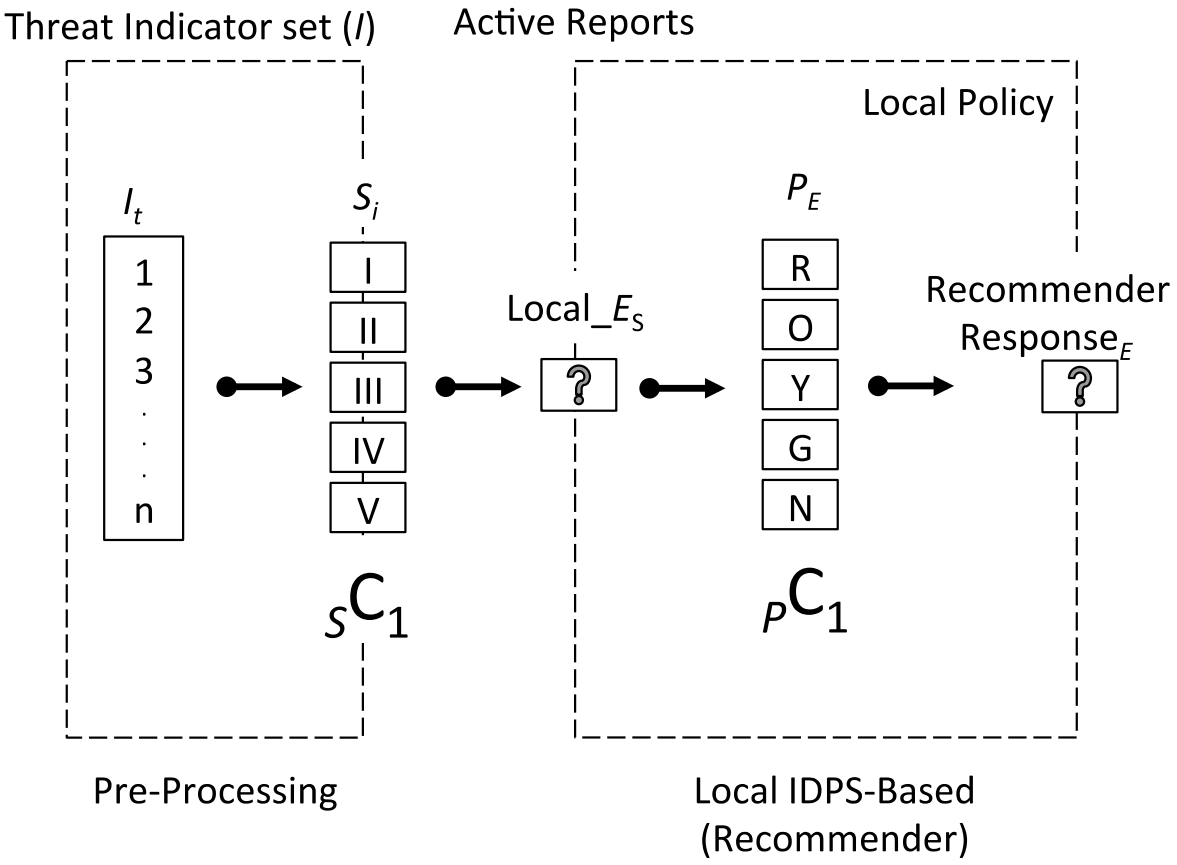

Figure 4. Conventional Threat Event Recommender System Scheme

The highlighted areas (Figure 5) show the two primary differences that Lightning has over the conventional method. The first highlighted difference shows *r* participating IDPS, which provide the local truth of the locally detected threat label event. The participants' threat reports and the local IDPS threat report are combined into the set of total threat indicators as the stimuli input. If participants share the same threat distribution (i.e. KDD99), the locally determined threat label can be represented by the same encoding scheme.

If participants do not share the same threat distribution of possible threat labels, then the local LAN must be able to distinctly map each label report received from a participant. As a result, the local decision-maker maps exactly one threat label to one of the five threat-severity levels (e.g. I, II, III, IV or V) during the pre-processing stage. In this way, the local decision-maker has a standardized rating scheme for all reported threats regardless of the originating source. In the pre-process stage for the GTERS model, instead of having a single threat label status to evaluate, the decision-maker evaluates all of the reported threat labels events from participants and its local IDPS as a single threat situation event.

Depending on the event and the locally defined DSP strategy to mitigate the threat, the local response policy is defined as a desired protective posture level (PPL). Each combined event occurrence is evaluated and a decision is made to respond with the best PPL. The PPL is submitted to the ANN for off-line learning, which produces the ANN structure and global response policy. After training is completed, the conventional IDPS is employed within the network security boundary (i.e. network edge), while the GTERS is employed within the management network to receive the participant's local IDPS outputs as the global event input. For each local participant the global input event is assessed against the ANN's learned global response policy, and based on the link weight structure, the ANN makes the PPL.

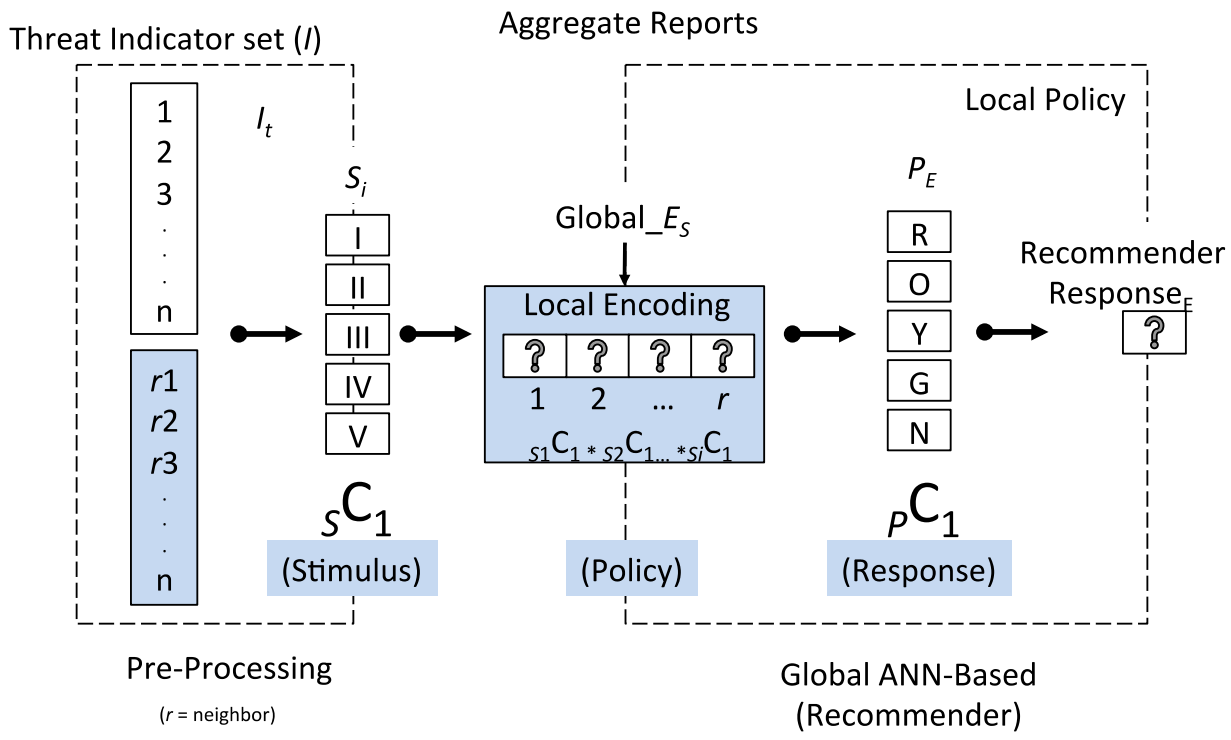

Figure 5. ANN-Based Global Threat Event Recommender System

After the DSPs are learned, which includes the process of assigning any neighbor reports into an associated Threat-Severity Level, the ANN can now be employed in an operational environment. Now, as threat events occurs from the local IDPS and neighboring IDPSs in the form of an aggregated global event stimulus, the learned set of local DSP policy's desired responses are provided by the ANN as PPL recommendations. Lightning (SUT) is a decision-support recommender system that provides a best-fit protective posture level (PPL) to local decision-makers performing duties in the network security and defense operational environment. The workload for the SUT (Figure 6) is the set of local IDPS reported events that occur after off-line training of the DSPs have been determined during preprocessing. The Local Decision-Support Profile (DSP) (Figure 7) is the first component under test (CUT) that provides input to Lightning during the Off-line phase.

The Off-line CUT is the second input for Lightning, which produces the global policy (Figure 8) that determines the protective posture level (PPL) recommendation. The recommended PPL, based on the detected global event threat pattern, is the final output of the GTERS. The system parameters and critical factors of the system appear along the top of the block diagram. Each Local area utilizes a primary IDPS to report and receive local events to and from the ANN.

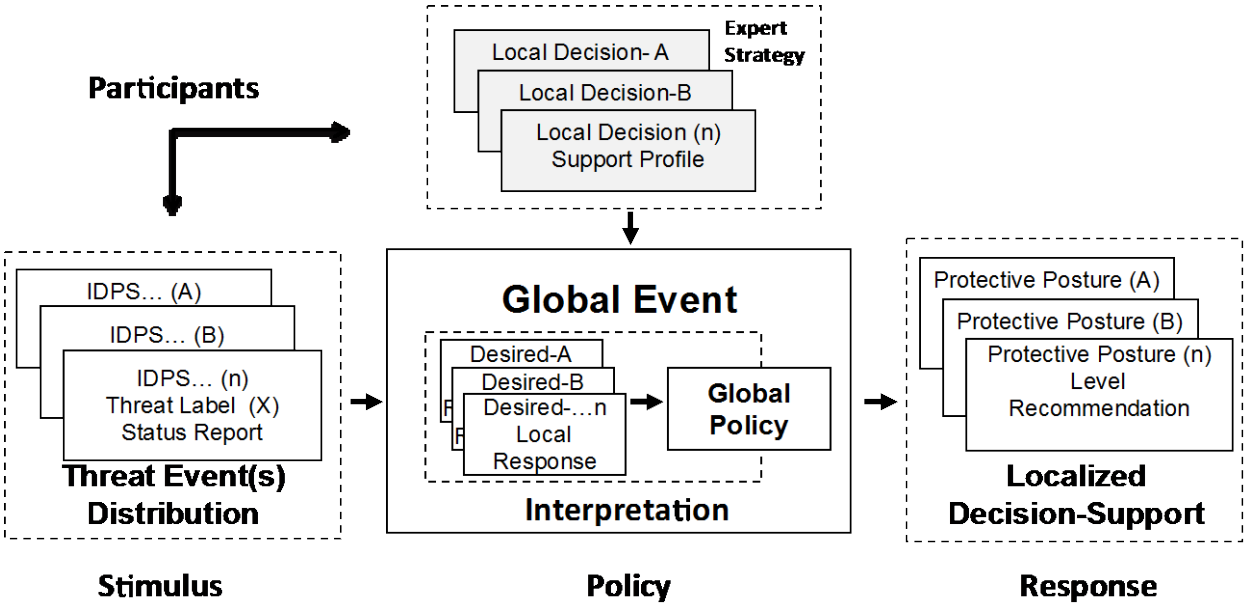

Figure 6. Lightning's Operational Block-Diagram

A PPL is the protective posture level that a local network boundary assumes in order to mitigate an actual or perceived threat event. For example, a PPL of "RED" as shown in Table 5 has the highest cost for an *imminent* threat. A PPL of "ORANGE" has a local interpretation of a significant threat has occurred or is highly likely to occur in the near future. The artificial neural network results provide independent posterior probabilities of threats that have occurred, and do not predict future threats in this model instance. It is assumed in this research that participants will participate and share threat characteristics called metadata.

This research defines metadata as the minimal amount of communicated data from a reporting IDSP to participating neighbors that describes the nature of the threat report. The meta-data is sufficient for participants to be able to interpret the threat label, not the contents of the reported event.

For example, if a hacker attempted a known signature pattern that resembles a *rootkit*, then a reporting IDPS can send a report that summarizes the time, type and location of the threat label, but does not transmit the offending contents of the detected pattern. The PPL is determined by the process of conducting a local risk assessment of each threat label or indicator based on the impact to maintain, recover from or continue normal business operations, goals and objectives despite the event.

In this research, threats are locally defined, but represent malicious or unwanted network traffic. This research adopts the general definitions used in the KDD99 dataset to establish a normalized distribution of global threats. For example, a *smurf* threat label is defined by the KDD99 dataset as a Denial of Service Attack, and it fall into the Threat Severity Level Category of Type-III attack. The baseline profile assigns this Type-II category defined by KDD99 to be interpreted as a Type-III Threat-Severity Level rating for the *smurf* threat label. A *rootkit* would be assigned as a local Threat-Severity Level of Type-I. A Type-I has the priority for mitigation and response actions. In this way, each participant assigns a Threat-Severity Level rating for each KDD99 threat label prior to submitting a DSP to the ANN for learning.

Table 5. Protective Posture Level Operating Cost Adapted from (Defense, 2001).

Protective Posture Level (PPL) Response Action	Operating Cost	PPL Response Action Description
RED (Imminent) deliberate	Extremely High	The local IDPS's reported status of an active threat or a preconfigured sequence indicates an imminent threat that could cause significant loss to *mission-critical* resources. This PPL requires **deliberate** threat mitigation and avoidance actions. To, reduce potential losses, IAW policy, you should: o Immediately deploy QRF resources to contain and mitigate this threat. o Significantly restrict all in-bound traffic flow o Conduct deep packet inspections of in-bound *mission-critical* traffic o Update active '*watch-list*' o Remain vigilant for near-term/future/persistent threats o Monitor, detect and report status to meet organizational goals
ORANGE (Significant) specific	High	IDPS(s)'s reported status of an active threat or a preconfigured sequence indicates a significant threat to *mission-critical* resources. The threat is not detected by local IDPS; however, additional credible information indicates a correlation that you may still be locally vulnerable to this active threat in the near-term. This PPL requires **specific** threat mitigation and avoidance actions. To, reduce potential losses, IAW policy, you should: o Place QRF resources on standby o Slow in-bound traffic flow for *mission-critical* resources o Random deep-packet inspections of inbound *mission-critical* traffic o Update active '*watch-list*' o Remain vigilant for near-term/future/persistent threats o Monitor, detect and report status to meet organizational goals
YELLOW (Moderate) random	Medium	IDPS(s)'s reported status of an active threat or a preconfigured sequence indicates a moderate threat to locally protected resources. This PPL requires **random** threat mitigation and avoidance actions. To, reduce potential losses, IAW policy, you should: o Random threat mitigation actions (i.e. QRF alert-recall, off-peak deep packet inspections, other access control audits.) o Modify pace of specified in-bound traffic flows o Update '*watch-list*' o Remain vigilant for near-term/future/persistent threats o Monitor, detect and report status to meet organizational goals
GREEN (Minimal) normal	Low	IDPS(s)'s reported posterior probability of an actionable threat was not sufficient for the employment of additional threat mitigation resources during this period. This PPL requires **normal** threat mitigation and avoidance actions. To, reduce potential losses, IAW policy, you should: o Update '*watch-list*' o Maintain normal operations for the next period. o Monitor, detect and report status to meet organizational goals No additional resources are deployed.

The KDD99 dataset is locally assessed by taking each possible threat label identified (Table 6) and configuring the IDPS to monitor detects and responds to the occurrence of the threat label when detected during normal operations. This is a critical step and should be conducted by a subject matter expert capable of assessing the threat event's perceived or actual impact to the organization's goals and objectives and protected resources.

Table 6. KDD99 Threat label Category Definitions (Hettich & Bay, 1999)

KDD99 Threat Label	Category Description/Definition
buffer_overflow	Unauthorized access to a local *superuser* or (root) privileges.
loadmodule	
perl	
rootkit	
ftp_write	Unauthorized access from a remote machine.
guess_passwd	
imap	
multihop	
phf	
spy	
warezclient	
warezmaster	
back	Denial of Service
land	
neptune	
pod	
smurf	
teardrop	
ipsweep	Probing: Surveillance and other probing.
nmap	
portsweep	
satan	
normal	Normal Traffic

A local area must conduct a threat assessment that best meets the objectives of their local goals and objectives (Pipken, 2000); The KDD99 dataset is used as a standardized threat distribution of threats, which establishes a common threat pool for this research. A Type-I event imposes the highest associated cost to mitigate a threat and presents the greatest adverse impact to a local organization. As participants report the status of globally occurring events, Lightning first aggregates the reports of event and then provides a localized best-fit PPL recommendation that most closely matches the learned decision maker's desired response.

A PPL determination is made based on the local decision-making strategy of minimizing the cost of threat mitigation. The organizational strategy to achieve a winning end state in Cyberspace depends largely on the interests, goals and objectives of the specified organization.

The organizational strategy provides the stimulus for open-loop emergent behavior, designed to achieve the end result of the strategy by employing methods.

The methods (i.e. tactics, techniques and procedures) employed to achieve the organizational goals will be collectively called the local policy. The local policy provides operational guidance to network security professionals as they employ tactical network security boundary defense operations. Collectively, the organizational goal, objectives, and local policy are called the local decision-support profile (DSP). Each DSP is locally determined during pre-processing for the GTERS by an expert network security professional. The SUT learns what the expert would do in threat situations and recommends threat mitigation and avoidance responses to novice defenders in uncertain situations.

The remainder of this chapter has four parts. A discussion of the general problem is revisited from Chapter I followed by the experimental problem. After the problem statement has been provided, two research goals are presented. The hypothesis is provided before the methodology. The methodology section discusses the system boundaries, scope, limitations, services, workload, performance metrics, parameters, factors, evaluations techniques, experimental design, and scenario development.

3.1 General Problem Review

Modeling Cyberspace as a CAS is a hard problem. Understanding the definition and context of Cyberspace, for a local interpretation can often be just as difficult. It is the local entity or individual's interpretation of the conceptual meaning that matter most. The capability to interpret larger concepts into local meaning drives the ability to obtain good situational awareness.

When decision-makers have good SA, they tend to make better decisions. A question of how two entities interpret the same global event that results in opposite decisive actions provides insight into how the aggregation of large data can be reduced to information of interest to a local entity. Humans are typically well adapted to filtering out things of interest and providing a localized interpretation of the interesting element's meaning.

A computer on the other hand, is well suited to find, detect and report the status of items of interest as defined by humans, but does not perform well with initial filtering of aggregated data because it contains no context cues. This makes the task of providing DSSs more difficult in dynamic and evolving environments where the meaning of interesting elements changes over time. DSS are well suited for problems where the environment or the element of interest amongst a world of noise remains relatively unchanged. Since Cyberspace is a CAS, the evolution of the meaning of an element of interest inherently evolves with the application of the meaning of Cyberspace.

The aggregate nature of Cyberspace has various applied contextual meanings to people, organizations and the military. The variations in the meaning of Cyberspace events and activities may lead to different decision-making responses when applied to obtaining goals and objectives. For example, a network that has been patched against a known *smurf* attack considers the presence of such a threat as a low threat event. Interestingly, this same event when applied to the context of a network that has not been patched against the threat will view the event at a higher level. Additionally, a windows-based network of devices may consider Unix-based threat events as low, while the Unix-based systems consider the same threat event as high. Although the detected event was identical, the meaning is determined locally.

As time goes on, the elements meaning evolves and new emergent behaviors arise for the DSS and the decision-maker. In the IDP, both the GTERS and the decision-maker must be in balance to monitor, detect and make appropriate responses for effective decision-making in the IDP. The decision-making process is an iterative planning methodology to understand the situation and mission develop a course of action, and produces an operation plan or order (Army U. D., 2005). Determining who, when, where, how, why and *what* to decide about a concept, or status of an element cue that may present opportunity to win or danger is a challenge in the decision-making process. Decision-support systems (DSS) in complex dynamic environments are also hard to develop because the knowing of *what* the DSS is conveying about a concept or status of an element cue to the decision-maker cognitive abilities is tough.

When the conveyance of meaning from the DSS is accurate, the process of appropriate decision-making may proceed, otherwise inappropriate decision-making may occur, or in the worst case, the DSS is no longer considered as a credible source of information in the decision-making process. The longer that it takes to assess the DSS, the longer it may take to make appropriate decisions.

A call for customizable DSSs that enhance the intrusion detection and prevention process for the local decision-makers has existed for a long time (BUI, 1986). A DSS differs from operations research methods in their stress on the interactive usability by computer-naïve decision-makers and in the intention of the DSS to provide support rather than fully automate the decision processes (BUI, 1986). Recalling the automation and optimization concerns addressed in Chapter II, there is a need to automate some data-mining and aggregation efforts, when the situation demands it. DSSs are often developed to facilitate well-defined sets of problems.

Modeling and simulating Cyberspace, as a CAS is not a well-defined problem due to the various interpretations of what Cyberspace means for a local network defender with respect to their organization's strategy to win.

The research aggregates local threat reports occurring across IDPS network security boundaries and applies the local interpretations of the aggregated event's meaning for appropriate response action consideration. The response actions, in this case are goal oriented, specifically to protect network resources from occurring attacks. This research focuses on the nature of the conventional IDPS reports that a network defender would assess, and takes each potential occurrence of a threat event and assigns a risk factor to it. The risk factor is calculated using a vulnerability rating adapted from the national vulnerability database (NIST, 2014), the Common Vulnerability Scoring System (CVSS) and Pipken (2000) Information Security principles.

The goal of minimizing cost to an organization by providing early warning allows mitigation and avoidance at lower levels of resource allocation. For example, Network A, may be immune to the *root-kit* attack, if it, had previously applied the patch against the threat signature. Because Network-A did not know about their vulnerability nor were they aware of the status of the threat (in isolation), they did not make an appropriate decision to apply a patch that other networks had. If Network-A could have obtained an element of interest from neighboring network sensor reports (i.e. an IDPS metadata report), then Network-A may have avoided the situation of allocating the highest levels of resources to thwart the attack.

Any level lower that RED benefits Network-A if mitigation efforts at this level are successful. The issue arises when the global threat does not occur locally and the local area has made a decision to allocate resources based on the global threat.

In this case, over time, the ANN can mature and additional training iterations can be made to overcome this situation where events have changed in local meaning. The overall goal is to model a simulated wide-area network employing ANN concepts to provide customized local decision-support to novice network defenders in an intrusion detection and prevention collaborations environment. To see how the attainment of this overall goal may emerge; the experimental problem statement, two supporting goals and the experimental hypotheses are presented next.

3.2 Problem Statement

How can ANNs, as CAS be employed to control emergent behaviors of integrated IDPS networks while providing SA and recommendations for local decision-support in Cyberspace? To address the problem statement, two primary research goals are made for this research objective. (1) Model and simulate a wide-area Artificial Neural Network-based Intrusion Detection and Prevention environment. (2) Validate the performance of a collaborative Artificial Neural Network recommender system for an interconnected IDPS environment. Having defined two primary goals of this research, the hypothesis is presented next.

The research hypothesis is that local decision-support can be enhanced by employing an artificial neural network-based event recommender system in intrusion detection and prevention environments. This research introduces this recommender system as a global threat event recommender system (GTERS), which aggregates the reports from disparate IDPSs and recommends a threat mitigation protective posture level based on local expert interpretation of the global event.

3.3 Experimental Methodology

A simulations approach is employed to meet the goals of this research. Lightning has two primary inputs as the components under test (CUT) called: Decision-Support Profiles and Off-Line training. Lightning's output provides localized protective posture level (PPL) recommendations to participants. Lightning's generalization accuracy to classify unseen patterns is assessed using the k-fold cross-validation method, where fold-9 is used as the final validation test.

The PASS/FAIL accuracy of Lightning's recommendations are assessed using the mean squared error (MSE) and overall PASS rate of the system given a training dataset and a set of distinct DSPs. Back propagation along with gradient descent and K-fold validation are employed to establish the ANN structure's link weights to assess Lightning's performance levels. The simulation environment is developed to support a wide-area networking construct that incorporates a contextual mental model, SA critical element representation, and ANN recommendation. The mental model provides a conceptual perspective of SA interactions between local security boundaries.

A valid mental model is of high importance in modeling and simulations efforts of a CAS. SA Critical factors are identified to conduct the monitoring, detection and response functions of the IDP. After conducting pilot studies to ensure the simulations match expected analytical results, arbitrary decision-support profiles are developed for evaluation. A more realistic DSP is then developed as the baseline expert opinion dataset. The baseline DSP is treated with noise, 9-fold cross-validation and multiple distinct DSPs are trained simultaneously. The next section discusses the boundaries of the system.

3.3.1 System Boundaries

Lightning aggregates globally occurring threat reports and provides localized decision-support to network defenders with a recommended PPL that was determined by their expert DSP development. Artificial neural network (ANN) concepts are employed to enable threat collaboration and assess decision-support capability across disparate network security boundaries.

The simulation enables group collaboration and information sharing across wide-area network security boundaries and recommends appropriate protective posture levels for local threat mitigation. Lightening enables group collaboration across network security boundaries by encoding local threat reports and distributing events to participants in real time. The scope, limitations, and system services including the workload, metrics, parameters, factors selected, the performance evaluation methods, and the experimental design are presented next.

3.3.2 Scope and Limitations

Lightning is a proof of concept modeling and simulation effort. The scope employs ANN technology across simulated wide-area networking environments. The modeling and simulation approach does not evaluate the security mechanisms, nor does it attempt to define trust establishment schemes. The modeled threat is externally originated and the management backbone is considered secure between networks. This research limits the scope of intrusion detection of incoming network traffic and that is directed to protected *critical-resources*.

Finally, the risk factor and risk assessment of potential threat events have been conducted during the preprocessing stage for each participant during DSP development.

3.4 System Services

Lightning classifies globally occurring threat event patterns and provides local decision-support recommendations to mitigate current or perceived near-term threats. Lightning provides a PPL recommendation based on the perceived threat severity inputs. The DSP CUT and the Off-Line CUT services are highlighted next.

3.4.1 Decision Support Services

The purpose of the DSP is to provide the ANN a target concept to learn the local DSP. The goal of the ANN is to classify occurring events and recommend a PPL to the local-decision maker that best matches their DSP strategy (Figure 7). The pseudo code for determining the DSP strategy is provided in Table 7. A DSP survey was prepared to collect a representative set of training data for this research. The DSP survey (Appendix A) is a four part anonymous study to determine the effects of event collaboration on human decision-support profiles. When faced with two network threat scenarios, respondents are expected to recommend a protective posture that best protects their local-area network security boundary. During Part I (Respondent Background), the respondents are asked to provide their closest matching IA work role and are introduced to the concepts and materials used during the study.

In Part II (Isolated Threat Mitigation Model Scenario-I) the respondents are asked to respond to the available threat reports while isolated from threat collaboration with other outside sources. The event sequence is repeated in Part III (Collaboration Threat Mitigation Model, Scenario-II), however the respondents are now authorized collaboration of threat reports with credible/participating neighbors from a wider-area about the threat event's occurrence.

Finally, in Part IV (Participant Reflection) questions are asked to determine if there was a decision-support profile change. Following the closing of the survey, respondents are asked to participate in an after action review. The survey is found in Appendix A.

Each local area can have independent desired responses for each DSP strategy profile input to the ANN. Because the output nodes are independent and each participant has its own localized set of output-nodes, each DSP strategy learned by the ANN will have an independent response output. This is important, since the ANN structure builds a separate set of link weights for each participant in this research. As the network grows, scaling concerns may arise, in this case, advanced group membership may provide cost saving benefits.

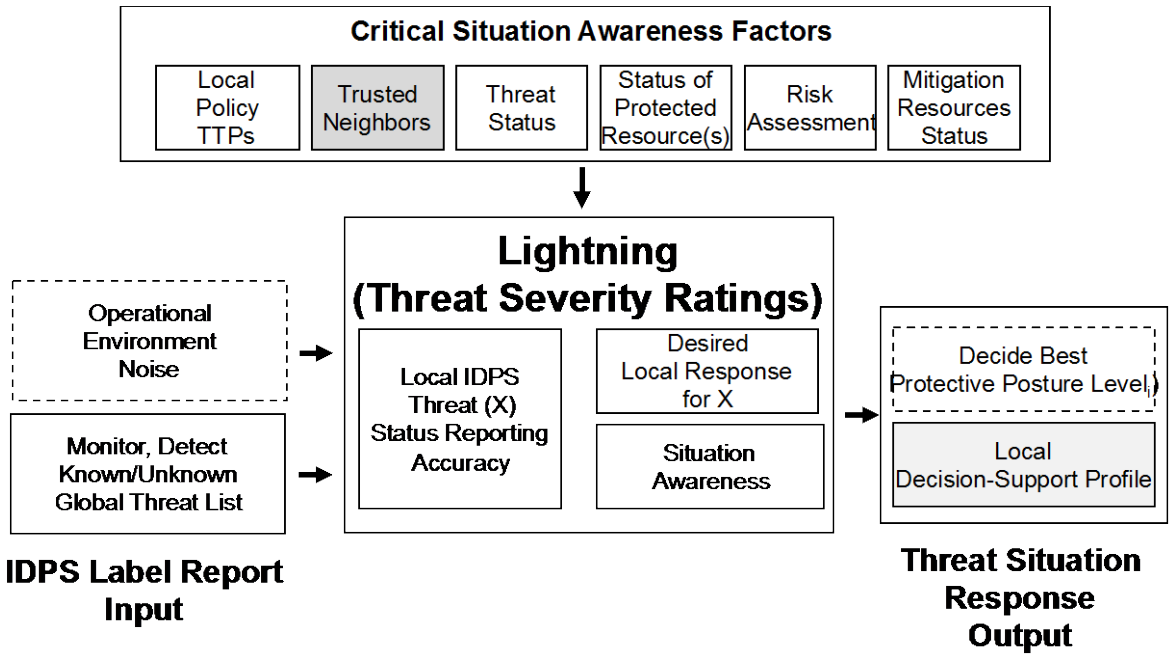

Figure 7. Local Decision-Support Profile Component under Test (CUT)

Table 7. Determining Local Decision Support Profiles (DSP) Strategies

Decision Support Profile Group Policy Inputs to the SUT
Initialize Group Formation(s)
Given:
- ANN interconnected IDPS across a wide-area networking boundary
- Subset of all Threats of Interest to participant pool
- n_Credible Participants
- Local Area network Security Boundary
- IDPS sensors interconnected with participants

// A Global event is the set of threat reports received by all participants during the reporting period

Develop Global Report Monitoring Policy:
For Each Local Participant:
Observe Local Policy Goals and Objective
For each reported (Local, Global) threat event combination
Conduct Risk Assessment
Return Risk Factor for each Threat-Event_x

For each (Risk Factor, Threat-Event_x) pair
Assign Threat Mitigation priority Severity Rating
Choose one-of L Severity-ratings
Return Severity-Rating one-of (e.g. I, II, III, IV, V)

For Each (Severity-Rating, Threat-Event_x) pair
Assign Most Likely Protective Posture Level (PPL)
Mitigation Color Code Category (e.g. Red, Orange, Yellow,)
Return Desired Local Mitigation Response
Return Local Decision Support Profile (DSP)

Return Global Policy set of desired local (DSPs)

3.4.2 Off-Line Services

The Off-Line training CUT (Figure 8) is also a critical input to Lightning and provides the link weight structure of the ANN's global policy. By learning the set of set of link weights that best minimizes the error in the system off-line, Lightning is positioned to provide a best-fit PPL recommendation for each desired response indicated in the DSP dataset.

The output of the Off-Line CUT provides the global policy and set of link weights for the ANN structure. The global policy is the aggregation of threat patterns as a detected event. The ANN's link structure detects the occurrence of a global event pattern and makes the best-fit PPL recommendations as events occur.

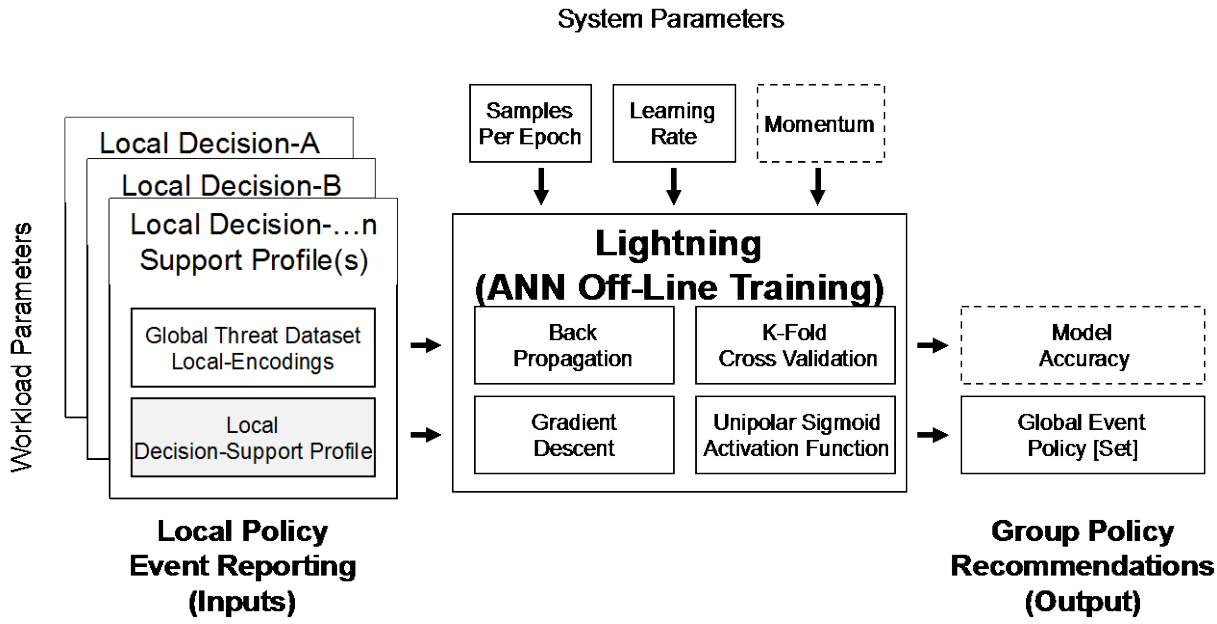

Figure 8. Lightning's Off-Line Training Parameters

In the learning phase, the local goals, objectives and policy guidelines are observed. In the Orient phase, the threat indicators where known or perceived is assessed and mitigation strategies are applied. When mitigation strategies such as patches have been applied to mitigate some threats, a residual risk factor is calculated. Table 8 shows the 10% KDD99 threat probability distribution summary. For each threat label, the KDD99 category, count and occurrence rate can be found. The 10% KDD99 dataset consisted of 494020 total events. 80.3% of the total events containing attack labels and only 19.69% of normal traffic.

The occurrence rate of each KDD99 threat label is used as the likelihood of occurrence to calculate the risk factor for each threat. The probabilities are taken for each threat and a risk assessment is conducted based on the perceived impact to protected resources for each label. The result of initial risk assessment provides a risk factor value.

For example, if organization X was in the business of providing real-time broadcasting services, then a potentially high-risk threat from the KDD99 dataset might be a *smurf* attack. A *smurf* attack is a denial of service attack according to the KDD99 category definitions. If organization X conducts an inventory assessment for their IDPS devices, they may rate them on a scale from 0-1, with a 1 being the most valued resource to the organization's ability to maintain normal operations and a 0 being the least valued resource to the organization for maintaining normal operations. For this example, organization X has rated a protected resource R with a value of 0.9. Organization X obtains information that a *smurf* attack has a 56.86% chance to be attempted against resource R. Using Risk Factor Calculation (Pipken, 2000), the local network defender for Organization X calculates the risk factor as:

$$Risk\ Factor_{threat\_n} = value_{resourcei} * P_{threat\_n} \quad (1)$$

In this case, we have a calculated risk factor value of (0.9 * .5686) = 0.51174. The overall risk factor for this example can now be used to recommend a proactive threat mitigation response in light of the calculated risk factor. The risk factor is associated with a Type-III Threat-Severity category (Hettich & Bay, 1999). Table 9 provides the complete risk factor mapping to protective posture levels.

Table 8. 10%KDD99 Threat Labels and Category Statistics (Hettich & Bay, 1999)

KDD99 Threat Label Distribution			
Name	**KDD_Category /Threat-Severity Level**	**count**	**Likelihood of Occurrence Rate**
back	III	2203	0.4459334%
buffer_overflow	I	30	0.0060726%
ftp_write	II	8	0.0016194%
guess_passwd	II	53	0.0107283%
imap	II	12	0.0024291%
ipsweep	IV	1247	0.2524189%
land	III	21	0.0042508%
loadmodule	I	9	0.0018218%
multihop	II	7	0.0014169%
neptune	III	107201	21.6997288%
nmap	IV	231	0.0467592%
normal	V	97277	19.6909032%
perl	I	3	0.0006073%
phf	II	4	0.0008097%
pod	III	264	0.0534391%
portsweep	IV	1040	0.2105178%
rootkit	I	10	0.0020242%
satan	IV	1589	0.3216469%
smurf	III	280790	56.8377798%
spy	II	2	0.0004048%
teardrop	III	979	0.1981701%
warezclient	II	1020	0.2064694%
warezmaster	II	20	0.0040484%
		494020	100.0000000%

In this research, the desired PPL would map to the local DSP. For example, if a Type-III threat label was not of interest to a local area, then they may recommend a PPL of ‘GREEN” or “NORMAL.” If a desired PPL response of GREEN or Normal was actually indicated by a local decision maker for this same threat indicator of *smurf*, it may convey that the threat element is a locally determined Type-IV or Type-V priority threat-severity level.

The same *smurf* event has occurred despite the locally determined Threat-Severity Level and PPL mapping. The ANN leans the desired response given the event as interpreted by the local decision-maker.

Table 9. Threat Risk Factor Mapping to Threat-Severity Level (Pipken, 2000)

Risk Factor --> Threat Seveity Level Mapping	
.8 - 1	I
.6 - .8	II
.4 - .6	III
.2 - .4	IV
< .2	V

Ideally, the threat categories would be evaluated via a survey. However, in this study, the risk assessment was conducted by the author and the risk factors were categorized by priority into five severity-levels adapted from the KDD99 category ratings of Type-I though Type-V. An additional consideration is made for designated mission critical resources.

3.4.3 System Workload

The DSP workload is the 10%KDD99 dataset (Hettich & Bay, 1999). The workload provides a common Threat Distribution dataset for local interpretation of participant's local IDPS threat reports. The output of the DSP CUT is a set of locally defined set of desired PPL responses that would best minimize threat mitigation. The Off-Line CUT is the set of DSPs that are presented to the ANN for learning. The result of processing the DSPs is the global policy set of link weights for the network structure.

3.5 System Performance Metrics

System success is measured by PASS/FAIL, where a PASS occurs when the recommended PPL from Lightning matched the associated desired response from the DSP. A score of FAIL occurs when the responses do not match. The Global policy output from the Off-Line CUT will be assessed using the cross-validation method. The average success rate is taken for all participants. Success is achieving at least 80% PASS from all participants.

3.5.1 System Parameters

The system parameters for each block diagram can be seen at the top of the diagram. The 18 parameters considered for the SUT are local policy, trusted neighbor status, threat status, protected resource status, threat risk assessment, available resources, the operational environment and the local-decision maker's confidence in the IDPS performance levels. Each parameter is described below.

1. *Local Decision-Support Profiles:* Decision-Support profiles are preprocessed during the training phase (Section 3.6). Once selected, the links weights of each desired response are maintained throughout the experiments. The more neighbors that report a locally defined threat severity match, the higher the contribution for the reported PPL recommendation.

2. *IDPS Threat reporting rates*: The rates of locally detected threats are workload inputs. Each Local Area has independent arrival rate distributions of normal, Poisson or exponential traffic patterns.

3. *Trusted Neighbors:* If neighbors are trusted, then the threat reports that match locally defined threat severity are considered for the recommended PPL output. If neighbors are not trusted, then the Local Area's desired responses do not consider any neighbor participation of reported threats. In that case, the PPL recommended is only the result of the individual decision-support profile.

4. *Seed Value:* The seed is the value used by NetLogo to maintain reproducible results during runtime. The input-nodes represent the Level-1 and level-2 SA element cues. There are 20 input-nodes used throughout the performance tests.

5. *Output-Nodes:* The number output nodes represent the encoded representation of the recommended PPL. In the pilot study, the choice is 1 out-put node per area and Scenario II and III use five out-put nodes for each area to interpret the encoded global event vector.

6. *Activation Function:* The Uni-polar Sigmoid Activation function (i.e. Logistic Function). The sigmoid activation function can be used with or without a threshold and provides a continuous output value between 0 and 1.

7. *Threshold:* The threshold is set at 0.5.

8. *Local Policy:* Local Policy, Tactics Techniques and Procedures: These parameters were chosen because they are critical elements in decision-making to support the organizational goals, guidance and specified directives that local decision-makers follow. Restrictive local policy constraints may lead to undesirable Global Policy generalizations and may provide undesirable recommendations to the local decision-maker.

9. *Threat Status:* This factor was chosen because it reflects Level-1 SA about *what* the threat element is doing in the operational environment, which is a critical factor for IDP. The IDPS and ANN detect the occurrence pattern of threats to make recommendations on the status of reported events.

10. *Protected Inventory/Resource Status:* Status of Protected Resource(s): This factor provides Level-I SA about *where* the threat event is occurring to local decision-makers.

11. *Risk Assessment:* Depending on the local area's residual risk factor, the desired response is affected to receive a higher recommendation or increased protective posture, if a global threat matches the local threat severity level.

12. *Mitigation Resources Status:* Local decision-makers may consider the time it takes to employ quick reaction forces to implement their highest level of threat mitigation and avoidance resources. Early warning Reponses can be recommended by desiring more responses for this particular threat despite the number of neighbors reporting.

13. *The Operational Environment:* The operational environment provides context and overall SA. Local decision-makers cannot make decisions based on things that they do not know; perhaps interconnecting network boundaries will reduce uncertainty.

14. *IDPS performance/Confidence:* Performance statistics of the reporting IDPS: Poor accuracy of the reporting IDPS will lead to a lack of trust in the system, and a loss of credibility for all participants in the global collaboration pool. These values are modeled, but not modified during this research.

15. *Run Time:* The runtime is the total amount of training periods that are used to train the ANN.

16. *Examples per epoch:* Each training sample is presented from the set of DSP to the ANN to learn how best to classify the desired response. The ANN has a greater chance of learning the correct classification of a sample, when the sample is presented multiple times. This desirable effect has an unintended consequence of reducing the generalized accuracy, so a balance must be found to reduce over fitting. A lower level can increase the generalization capability of the ANN and approximate the classification of unseen samples when placed in the online performance mode. Cross validation is commonly used to find this balance.

17. *Learning Rate:* The learning rate for the ANN is used to adjust the step size when distributing the error across the system and tune the link weights so that the desired response matches the actual response with an acceptable level of accuracy. A high learning rate tends to allow faster runtimes due to larger increments (step size) in ink weight adjustments. A lower learning rate takes more time because link weights are adjusted in smaller increments.

18. *Momentum*: Momentum was not used as a parameter in this research. It is used to assist gradient descent to avoid providing link weight values found for the ANN that would represent a local minimum error.

3.5.2 System Factors

The learning rate and samples per epoch are critical factors for the training portion. Each factor has two levels, high and low. The samples per epoch factors are chosen because it represents how many times each sample is shown to the ANN during training. The goal is to minimize over fitting of the DSP training data and generalize the global policy for improved performance when Lightning is faced with unseen data.

1. *Number of Output-Nodes:* 1 used in the Pilot Study 5 output-nodes used in Scenarios II and III. This metric's purpose is to represent local PPL Levels. In the pilot study only one output node was employed to indicate that a Type-I threat had been detected. Minimums of three output nodes are required to distinctly represent the five protective levels used in scenarios II and III.

2. *Synthetic Data Levels (Noise):* On or Off. This metric was chosen to assess the performance of the ANN's accuracy when given noisy DSP and to perturb the DSP data.

3. *Cross-Validation:* On or Off. The purpose of the validation method is chosen to assess over fitting the training dataset and provide generalization accuracy for unseen threat events.

4. *Number of distinct expert DSPs:* 1 or 4 in all scenarios. This metric provides localized interpretations of the globally detected threat event. The research goal is validate the claim of independent DSP PPL recommendations when training the ANN with a single global policy.

6. *Learning rate:* .005, .3, .7 and 1.0. This metric is chosen to assess the effects on the ANN's performance using gradient descent and various step sizes.

5. *Runtime:* 10 epoch *ticks.* The low training periods are chosen to evaluate the performance given small training periods, which is desirable for dynamic operational environments.

6. *Examples per epoch*: 1. This factor was chosen to prevent bias of the ANN's learning from seeing samples multiple times in a single epoch. This metric's purpose is to prevent bias of ANN's learning from seeing samples multiple times in a single round.

7. *Number of input-nodes*: 20. This metric was chosen to support the threat Label encodings to Threat-Severity Levels. If each KDD99 threat label is to be distinctly encoded from participants, then an encoding value of 4 would not distinctly represent 23 labels from the KDD99 dataset.

Five input-nodes per area were employed to distinctly encode the KDD99 threat dataset. The label encodings are then mapped to a threat-severity level rating, followed by a PPL mapping according to the locally DSP.

The DSPs are treated with noise to assess the performance of the ANN's recommendation with noise environment in Scenario-II. The original Lewis-DSP dataset if modified to produce synthetic noise. The original dataset is divided into the five categories of threat severity ratings. Each category is then sorted randomly. 25% of the samples from each category are selected and treated. The treatment applies a 1-bit difference in the desired response column. For example, if the original desired response for sample ID 26 was encoded as [1 0 0 0 0], then this represented a Type-I category. It is recoded as a Type-II threat with the encoding [0 1 0 0 0]. After all of the sorted categories were treated, then all of the samples were then recombined into the modified noisy dataset. The recombined noisy dataset replaces the original baseline dataset DSP. The noisy DSP is presented as input to Lightning for global policy determination. After the off-line training has been performed for each desired response and combined threat situation event pair, Lightning is now ready for performance analysis.

3.5.3 System Evaluation Technique

The MSE, generalization accuracy and Pass rate are used to assess the SUT's performance. The MSE error is commonly used in training single layer feed forward ANNs (Heaton, 2012) and chosen here because we are using multiple output nodes and would like to obtain a total system average as well as a local average. The Pass/Fail metric (Higher is better): rate provides accuracy to recommend the correct PPL provided by the expert decision-maker. Where *D* is the training dataset:

$$Training_{Accuracy} = \frac{totalPass}{total_D} \quad (2)$$

Generalization accuracy (higher is better) provides a measure of the model's accuracy of correcting detecting and recommending the correct PPL when faced with unseen events/data accuracy.

$$Generalization_{Accuracy} = \frac{totalPass}{total_{hidden_{fold}}} \quad (3)$$

The Mean squared error metric (Lower is better) is the third measure of performance and provides the average error of the system. It is calculated using (Heaton, 2012).

$$Average\ system\ Error\ = \frac{\sum_{d \in D} \sum_{k \in outputs} (t_{kd} - o_{kd})^2}{k} \quad (4)$$

The simulation provides a 3D display of four independent networks using the NetLogo version 5.0.4 simulation tool. Packets are arriving to each LANs IDPS for processing and threat label determination. The ANN is used to interconnect the LANS using a separate interface on the IDPS for the Management network. Employing the ANN as the network communications backbone, all IDPS reports are sent to the SUT as input for processing according to the Global policy.

As each local area detects a threat, the threat type is indicated in Red. Each IDPS sends an "alert" encoded metadata threat report to the ANN by flashing a light. The flashing light indicates an active detected threat status during that period. At each *tick* step, the local IDPS independently reports the status of a threat to the ANN, and the ANN detects the globally occurring event. Based on global event, the ANN recommends the best PPL for each local area for threat mitigation decision-support. At the end of the testing, the simulation model computes the overall pass/fail rates and the success rate of matching the desired PPL response are reported.

3.5.4 Decision-Support Evaluation Technique

Each sample has a desired and actual response contained within the DSP dataset. The MSE is calculated during the training phase of the ANN. Generalization accuracy is a frequently used method in ANNs to assess the overall capability to classify items unseen by the ANN. The Cross-Validation results will measure the final generalization accuracy of the model.

3.6 Experimental Design

The experimental partial factorial design consists of three sections, the pilot study, DSP in noisy environments and multiple DSP effects on the ANN performance. All three studies use the developed simulations model using NetLogo for performance evaluation.

3.6.1 Pilot Study Design (Scenario I)

The pilot was study was used to familiarize with ANN concepts and develop the simulations environment. The study looks at a local instance of an ANN structure operating in parallel with a global ANN recommender policy.

For example, in sample_5 and sample_24 (Table 10), area A desires a PPL recommendation (indicated by a value of 1 in the column AO to mitigate a Type-I threat because at least 2 of its local devices have reported the detection of malicious traffic. All other areas do not desire a response for these possible global patterns. The pilot study only considered one type of threat, Type-I. A manual validation method was used during the pilot study. The working model can be found in Appendix D. The parameters used for the pilot study performance test are the same as described above except there is only output node for each local area. From left to right, the external stimuli are shown that can arrive to the ANN structure to one or more of the input nodes. The local area's target concept or desired response was leaned from arbitrary decision-support profiles using the m-of-n strategy.

Where n is the number of neighbor reports participating in the threat collaboration group, Area-A employed a strategy to recommended a PPL of "On" whenever there were at least 2-of-n neighbor reports of a Type-I threat. Area-B employed a 3-of-n strategy, while Area-C had a 4-of-n strategy and Area-D had a 5-of-n DSP strategy.

Table 10. Pilot Study-1 Initial Global Policy Dataset w/Errors

DATA SET X Errors1

		A							B							C							D						
Policy#	[	B	x0	x1	x2	x3	x4	D	x0	x1	x2	x3	x4	D	x0	x1	x2	x3	x4	D	x0	x1	x2	x3	x4	D	
0	[	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	[	1	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0
2	[	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0
3	[	1	0	0	0	1	1	1	0	0	0	1	1	0	0	0	0	1	1	0	0	0	0	1	1	0	0
4	[	1	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0
5	[	1	0	0	1	0	1	1	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0
6	[	1	0	0	1	1	0	1	0	0	1	1	0	0	0	0	1	1	0	0	0	0	1	1	0	0	0
7	[	1	0	0	1	1	1	1	0	0	1	1	1	1	0	0	1	1	1	0	0	0	1	1	1	0	0
8	[	1	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0
9	[	1	0	1	0	0	1	1	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0
10	[	1	0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0
11	[	1	0	1	0	1	1	1	0	1	0	1	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0
12	[	1	0	1	1	0	0	1	0	1	1	0	0	0	0	1	1	0	0	0	0	1	1	0	0	0	0
13	[	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	0	0	1	1	0	1	0	0
14	[	1	0	1	1	1	0	1	0	1	1	1	0	1	0	1	1	1	0	0	0	1	1	1	0	0	0
15	[	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	1
16	[	1	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0
17	[	1	1	0	0	0	1	1	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	0
18	[	1	1	0	0	1	0	1	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	0
19	[	1	1	0	0	1	1	1	1	0	0	1	1	1	1	0	0	1	1	0	1	0	0	1	1	0	0
20	[	1	1	0	1	0	0	1	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	0
21	[	1	1	0	1	0	1	1	1	0	1	0	1	1	1	0	1	0	1	0	1	0	1	0	1	0	0
22	[	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	1	0	1	1	0	0	0
23	[	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1
24	[	1	1	1	0	0	0	1	1	1	0	0	0	0	1	1	0	0	0	0	1	1	0	0	0	0	0
25	[	1	1	1	0	0	1	1	1	1	0	0	1	1	1	1	0	0	1	0	1	1	0	0	1	0	0
26	[	1	1	1	0	1	0	1	1	1	0	1	0	1	1	1	0	1	0	0	1	1	0	1	0	0	0
27	[	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1
28	[	1	1	1	1	0	0	1	1	1	1	0	0	1	1	1	1	0	0	0	1	1	1	1	0	0	0
29	[	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	1	0	1	1
30	[	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1
31	[	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
		B1	A	aR1	aR2	aR3	aR4	AO	B	b1	b2	b3	b4	bO	C	c1	c2	c3	c4	cO	D	d1	d2	d3	d4	dO	

The first column indicates the training sample_ID that was used to verify the ANN recommendations after training. Under the column heading 'B1' indicates the bias input node that is always set to the value of 1. After that a set of five values represents the five devices used for each local area's IDP defense structure. A value of '1' indicates that the device reported a positive detected element status of a Type-I threat in the reporting period, '0' otherwise.

The sixth value highlighted in green represents the local decision-maker's most likely choice that they would respond to this situation if it occurred. As a result of this, a value of '1' indicates that they desire a positive PPL recommendation from the ANN, '0' or no response is desired otherwise.

From left to right a logical representation of the simulations environment (Figure 9) depicts external stimuli arriving to the ANN structure to one or more of the input nodes. As a stimulus arrives to each independent area the set of input nodes are aggregated to provide the activation of the output node for each area. Each area's output node has a distinct and separate interpretation of the input stimulus value. In this way, each local area can interpret the stimulus as desired to meet their local policy goals and objectives. As a result, a local open-loop emergent behavior may occur from the global stimulus feedback. Global or feedback-loop emergent behavior results from the aggregation of the reporting input nodes as a learned global policy. The ANN recommends the PPL that best fits the local area's desired PPL response as the output. Each output node is a single and independent node for each area. Only Type-I threat labels are considered in the pilot study (either present or not).

Each Local area has five input nodes, with 1-primary IDPS (largest black node) at the network edge boundary. The primary IDPS provides the most significant level of decision-support to local network defender response actions. Each IDPS's reports are inputs to the SUT. Each LAN interprets the threat status using an m-of-n strategy. Area-A employs a 2-of-n Type-I detection DSP strategy. A 3-of-n, 4-of-n and 5-of-n strategy is employed for Area-B, Area-C and Area-D respectively. There are 32 situation events in the pilot study training dataset.

Given the five independent output nodes, 160 evaluations are performed on the 32 samples (5 local output nodes * 32 situation events). We establish performance on an error dataset vs. error-free dataset.

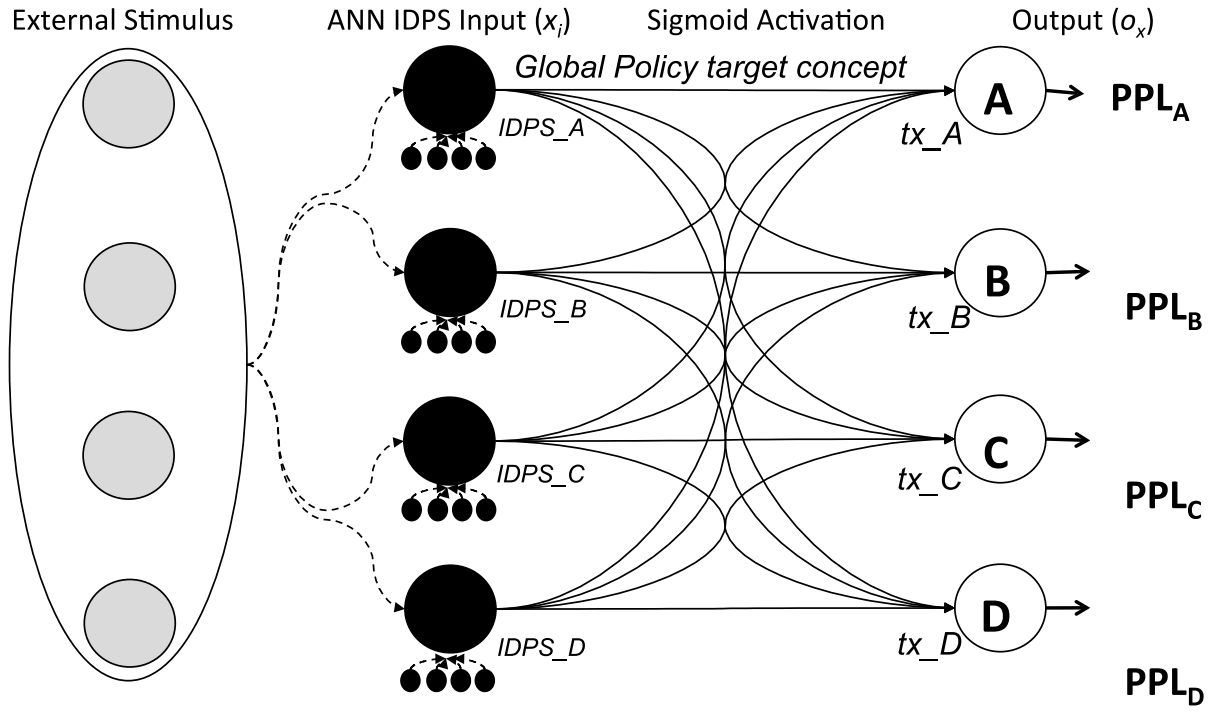

Figure 9. Pilot Study Logical View of 4-Area IDPS Integrated ANN Structure

3.6.2 Scenario II Single Decision-Support Profile Design

In scenario II, the modeling and simulations environment builds on the pilot study design. The arbitrary 32-sample threat distribution dataset is replaced with the 10% KDD99 dataset threat label distribution (Hettich & Bay, 1999). Area-A's DSP strategy is improved to reflect a realistic DSP network security strategy to include constraints. The DSP strategy for Area-A is the baseline DSP.

The baseline is treated with a 25% noise function and a cross-validation with noise treatment. Local Area networks: Areas-B, C, and D are active participants, but their DSP strategies are not considered in this scenario.

The Baseline DSP employs a total of five output-nodes to interpret the PPL recommendation from the ANN at each time step (Figure 10). The ANN receives 21 input nodes as stimulus for the network structure including the bias node. Each local IDPS has five input nodes that detect the KDD99 threat label, and sends the threat label to be mapped by the DSP into a locally defined Thereat-Severity-level. KDD99 dataset: Each randomly receives a normal distribution of the 23 threat labels. All 23 labels are prioritized into five locally defined threat severity level categories in the following order of priority; I, II, III, IV, V. Type-I categories have the highest priority for threat mitigation and avoidance actions. This allows each sample to have exactly four encoded reports and each report has 5 possible encodings yielding 625 total distinct samples. Each sample has a desired response associated for each Area. The Baseline DSP has five output nodes. The output nodes are designed to represent a five-digit encoded value. The desired response indicates the level of perceived threat severity that the reported samples pose to The Baseline DSP. Since each, sample is only shown to the ANN once for performance testing; only the perturbed data samples were added to the final data set. The DSP strategy is provided next.

The baseline dataset consisted of 625 samples. The validation method used the training data to test the performance of the SUT. The settings were consistent as described above using four learning rates.

Baseline Constraints: The Baseline DSP provides local policy induced constraints and does not desire a PPL recommendation of RED from the ANN unless the local IDPS has indicated a Type-I priority threat. The strategy is as follows: If the local IDPS reports a Type-I locally defined threat severity level, then the expert's desired response = PPL RED. Otherwise, choose m-of-n strategy for neighbors that report threat reports that are locally interpreted as Type-I as follows: If <1/3n report Type-1, then request PPL = Green/Normal. If Type-I reports > 1/3n < 2/3 request PPL = Yellow. If Type-I report >= 2/3n, request PPL = Orange.

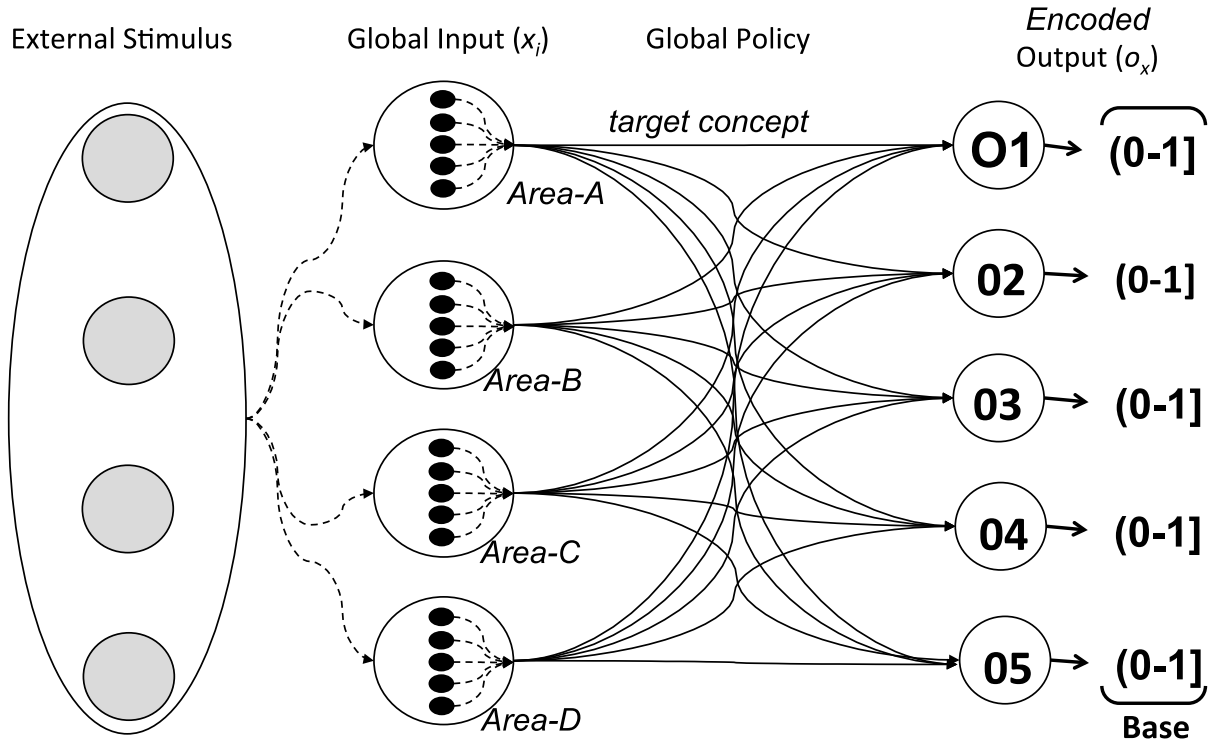

Figure 10. Logical ANN Scenario-II Performance ANN Structure

3.6.2.1 Scenario II Single Decision-Support Profile Baseline + Noise

The Noise dataset consisted of 780 samples. The validation method used the training data to test the performance of the SUT. The settings were consistent as described above using four learning rates.

Synthetic DSP dataset: In order to evaluate the SUT with more valid decision-support profile datasets, the *Baseline* DSP dataset was perturbed using the following method. 25% of all original RED responses were randomly sorted, selected and modified to an Orange PPL desired response. 25% of all original ORANGE responses were randomly sorted, and equally recoded as either RED or YELLOW categories. 25% of original Yellow desired PPL responses were randomly sorted, and recoded as either Orange or Normal categories. All perturbed data samples are indicated with a Label_ID as well as the original sample_ID number for manual error resolution.

3.6.2.2 Scenario II Single Decision-Support Profile Baseline+Noise+CV

The final setting for Scenario II used cross-validation on the noisy dataset using 9-fold Cross validation. A total of 105 hidden samples were presented to the ANN for performance assessment. The settings were consistent as described above using four learning rates.

3.6.3 Scenario III Group Decision-Support Profile Design

Building on scenario II's performance, scenario III introduced three new DSP profiles into the final ANN structure. A logical representation of the simulation environment for scenario III (Figure 11) adds an additional 15 output-nodes totaling 20 output nodes for the scenario.

Three DSP strategies have been added to the ANN structure, creating four sets of independent output node reporters for each area. Each area used a particular DSP strategy including the baseline strategy above.

The baseline threat distribution of 625 samples is used and now includes four sets of DSP desired response sets that are locally determined based on the globally detected event policy. Only one treatment is applied, 9-fold cross validation. Scenario-III is described next.

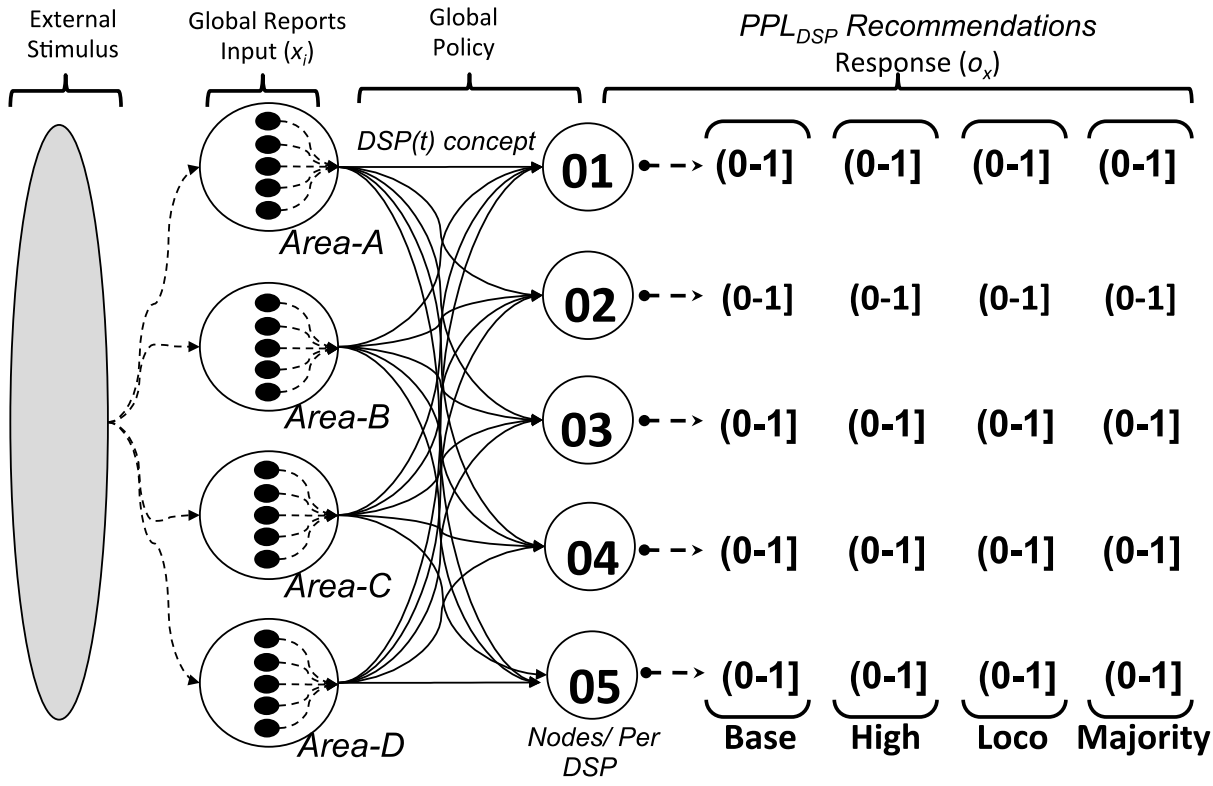

Figure 11. Logical Group Scenario-III ANN Structure

Baseline: (See section 3.6.2)

High-Roller: The high roller DSP desires a PPL recommendation that matches the highest locally interpreted IDPS threat label report as follows; Set desired PPL as the HIGHEST locally interpreted Threat Severity Level. (i.e. a report of a *smurf*, *satan*, *perl* and *warezclient* threats labels are detected for the global event, then using KDD99's category as local priorities, the highest is Type-I category for the *perl* threat, then PPL = Orange).

Local Only (LOCO): The LOCO DSP strategy desires a PPL response that matches the local IDPS for Area-C only. In this way, Area-C is acting as a reporter of threat events, but does not actively participate in the Global event PPL recommendations. The strategy goes as follows; Set Desired response PPL to equal local IDPS report only.

Majority Vote: The majority DSP uses a voting strategy approach to mitigate globally occurring threats. In the event of a tie, a random tie break is used to randomly sort the tied reports and then select one. The strategy is: Set PPL = majority vote of threat labels within the global event policy as interpreted for the local area. If a number of threats are equal in the matching number of votes, then conduct a random sort and select of one of the tying threats to mitigate. For example, if the following reports were provided [*phf, spy, rootkit, nmap*]. Following this DSP strategy, the desired response would have a Threat-Severity Level set of [II, II, I, IV]. The result is a Type-II Threat Severity-Level which corresponds to PPL = Orange. 9-Fold cross validation was conducted using the group baseline DSP dataset.

3.7 Methodology Summary

In summary, Lightning simulates an integrated ANN-based large-scale network security boundary operational environment that encodes local decision-support profiles of multiple participants, learns the desired response policy for each profile, aggregates the contribution of participant reports and recommends protective level responses using the learned global policy. The results are provided next.

IV. Analysis and Results

The results of the pilot study, Scenario-II and Scenario-III are presented in this chapter. The pilot study was used to conduct performance tests on arbitrary decision support profiles, while scenarios II and III built on lessons learned from each scenario.

4.1 Pilot Study Results

This research employed NetLogo to model and simulates a wide-area Intrusion Detection and Prevention networking environment using a single layer ANN as the backbone for communications. Using the manual validation method, several initial errors in the DSP dataset design were found and corrected. Despite errors, the performance accuracy of desired-observed pairs was 96.80% (Figure 12). Errors decreased from a high MSE of 3.34 using a 0.005 learning rate to a MSE of 0.52 using a learning rate of 1.0. This common trend of the performance accuracy leveling off with an approximate learning rate of 0.7 while the average MSE decreases with an increase in the learning rate step size is shown in all performance results.

Corrections were made to the dataset errors, and the error-free dataset is shown in Table 11. For example, the correct ANN PPL recommendations for all areas from the learned sample_7, which shows Area-A's and Area-B's positive desired responses, in red, were met in the global policy, while Area-C and Area-D's negative PPL response desires, in green, were also met for Type-I notification according to the global threat event recommender system. After correcting the errors manually using the performance accuracy of the model improved to 100.00% (Figure 13).

Table 11. Corrected 32-Sample Dataset errors

DATA-SET_Y_v2

G-Policy		2-of-5						3-of-5							4-of-5						5-of-5						
0		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1		0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	1	0	0
2		0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0
3		0	0	0	1	1	1	0	0	0	1	1	0	0	0	0	1	1	0	0	0	0	1	1	0	0	0
4		0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0
5		0	0	1	0	1	1	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0
6		0	0	1	1	0	1	0	0	1	1	0	0	0	0	1	1	0	0	0	0	1	1	0	0	0	0
7		0	0	1	1	1	1	0	0	1	1	1	1	0	0	1	1	1	0	0	0	1	1	1	0	0	0
8		0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0
9		0	1	0	0	1	1	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	0
10		0	1	0	1	0	1	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	0
11		0	1	0	1	1	1	0	1	0	1	1	1	0	1	0	1	1	0	0	1	0	1	1	0	0	0
12		0	1	1	0	0	1	0	1	1	0	0	0	0	1	1	0	0	0	0	1	1	0	0	0	0	0
13		0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	0	0	1	1	0	1	0	0	0
14		0	1	1	1	0	1	0	1	1	1	0	1	0	1	1	1	0	0	0	1	1	1	0	0	0	0
15		0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	0	0	0
16		1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0
17		1	0	0	0	1	1	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	1	0	0	0
18		1	0	0	1	0	1	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	1	0	0	0	0
19		1	0	0	1	1	1	1	0	0	1	1	1	1	0	0	1	1	0	1	0	0	1	1	0	0	0
20		1	0	1	0	0	1	1	0	1	0	0	0	1	0	1	0	0	0	1	0	1	0	0	0	0	0
21		1	0	1	0	1	1	1	0	1	0	1	1	1	0	1	0	1	0	1	0	1	0	1	0	0	0
22		1	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1	0	0	1	0	1	1	0	0	0	0
23		1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	0	0	0
24		1	1	0	0	0	1	1	1	0	0	0	0	1	1	0	0	0	0	1	1	0	0	0	0	0	0
25		1	1	0	0	1	1	1	1	0	0	1	1	1	1	0	0	1	0	1	1	0	0	1	0	0	0
26		1	1	0	1	0	1	1	1	0	1	0	1	1	1	0	1	0	0	1	1	0	1	0	0	0	0
27		1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	0	0	0
28		1	1	1	0	0	1	1	1	1	0	0	1	1	1	1	0	0	0	1	1	1	0	0	0	0	0
29		1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	0	0	0
30		1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	0	0	0	0
31		1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	
		B1	A	aR1	aR2	aR3	aR4	A0	B	b1	b2	b3	b4	b0	C	c1	c2	c3	c4	c0	D	d1	d2	d3	d4	d0	

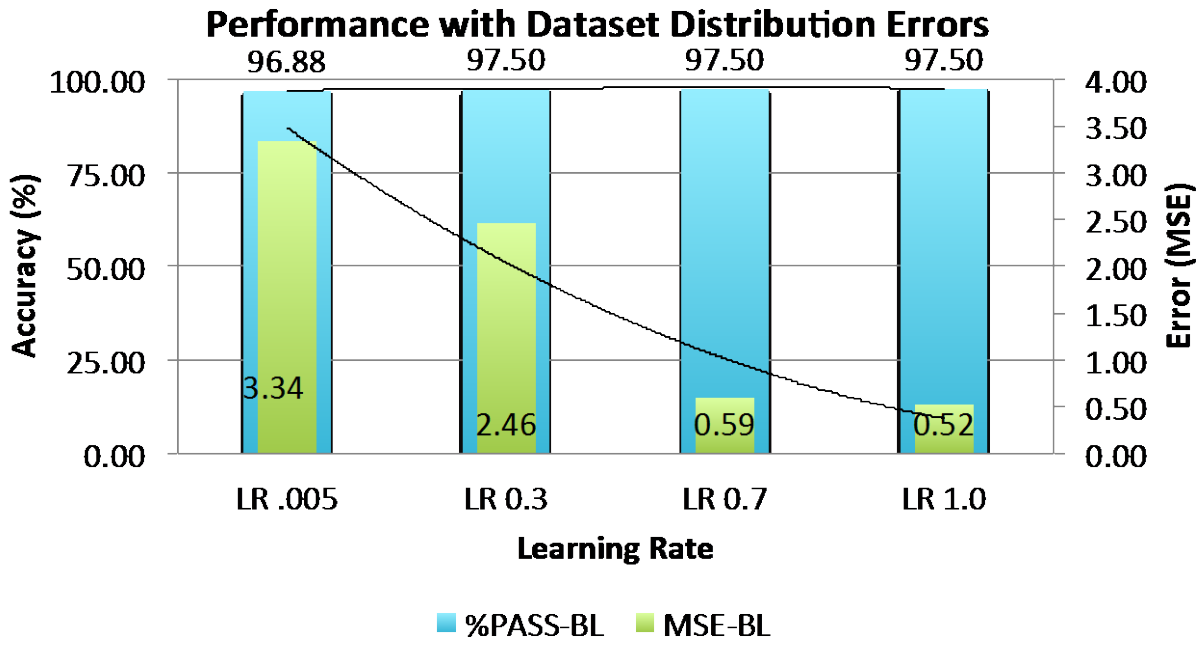

Figure 12. Pilot Study Results with Errors

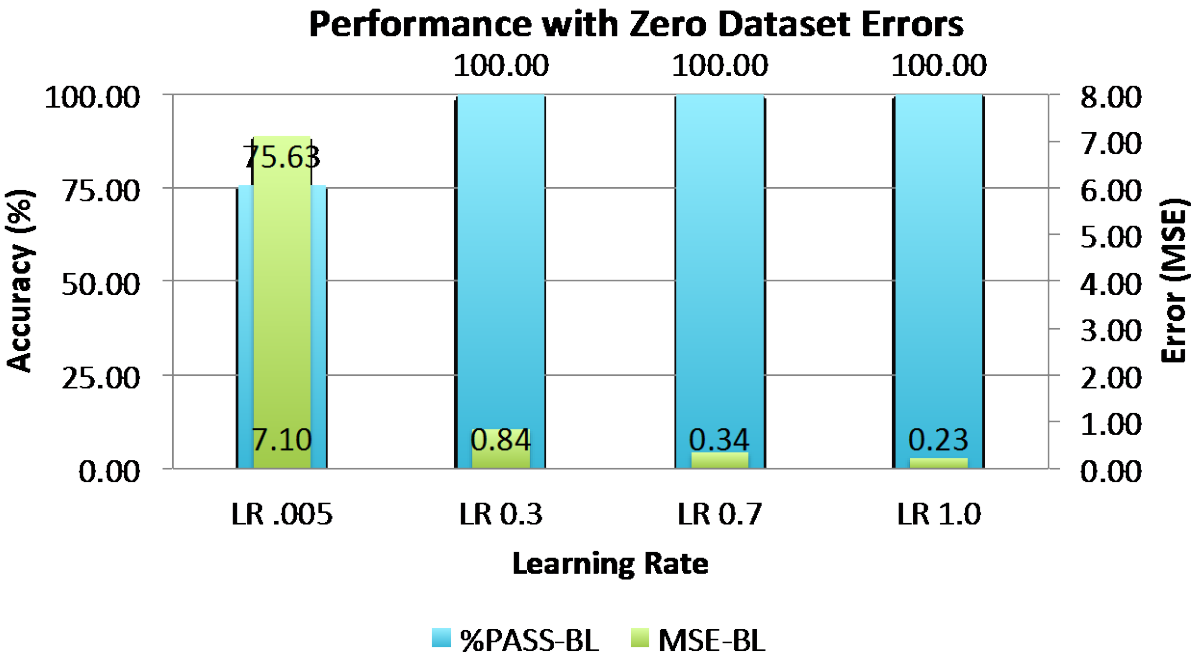

Figure 13. Pilot Study Error-Free Dataset Results

In summary the pilot study was used to establish the initial simulations mental model and operational environment in order to facilitate the performance evaluation of the SUT. The original dataset had multiple errors, which were due to incorrectly entered data. Prior to correcting the dataset the ANN recommendation accuracy was over 97.5%. An interesting discovery was made when all output nodes were trained to the same profile. The m-of-n strategy results demonstrate how an arbitrary DSP can be independently and simultaneously represented by a commonly shared global threat event recommender system, such as Lightning. Using an error-free training dataset, the ANN achieves 100% accuracy using a learning rate of 0.3.

4.2 Scenario II- Analysis of the effects of Noise and Cross-Validation on Decision-Support Profiles

In scenario two, DSP Profile_L1a_GO_5 was used as the PPL learning dataset combined with the 10% KDD99 threat label dataset. Each of the 23 threat labels defined by the KDD99 dataset falls into five categories and do not indicate a level of residual or actual risk to a localized area (Hettich & Bay, 1999). Each DSP rates the KDD99 distribution of threats according to the level of residual risk that remains after conducting a risk assessment as if the threat had occurred independently.

The threat distribution dataset consists of four encoded sets of data, which represent the final threat severity rating of The Baseline's interpretation of the 10%KDD99 report labels. The KDD99 dataset consisted of 625 normally distribution samples where each sample consisted of four sub events and each sub event consisted of one of five Threat Severity Level ratings for a KDD99 threat label categories. The samples were treated with a random 25% noise after the initial desired responses were made using the *baseline* DSP. (Figure 14) shows a summary of the baseline DSP performance results.

The baseline performance results used the 625 KDD99-based Type-Severity Level combinations for four participants. The validation test was conducted using the same training data. The performance accuracy is highlighted in blue and the error is indicated in green (Figure 14). The ANN PPL recommendations are 98%.02 accurate with a MSE of 13.82. The highest learning rate of 1.0 saw a slight decrease in accuracy for the ANN achieving a 97.02% accuracy rating, however it was higher than the lowest training rate's 88.20% accuracy level.

The ANN has a high success rate against data samples that it was trained on or previously *seen*. A low learning rate sees the highest error and achieves the lowest accuracy rating, and this is due to the nature of gradient descent taking smaller step sizes in an attempt to find the global minimum for the entire dataset. This is contrasted with the highest learning rate, which corresponds to a higher gradient descent step size. As a result, the error increases from the previous learning rate of 0.7. The optimal leaning rate for this dataset using this parameter is a learning rate of 0.7, which yields the highest accuracy and the lowest error. Interestingly, the 0.7 learning rate would also provide the worst performance for generalization of *unseen* or hidden data that the ANN was not trained on prior to establishing the final link weight structure for the network. In some situations where the patterns are relatively static in nature, achieving high training validation accuracy is desirable, however in dynamic environments; the ability to approximate unseen patterns is desirable.

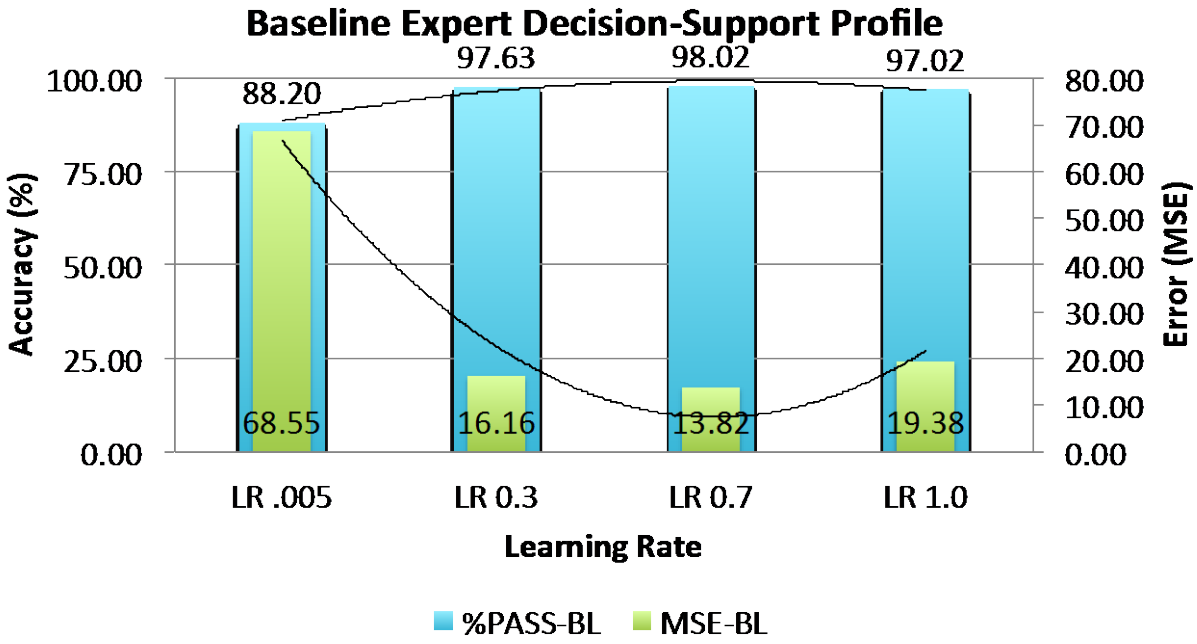

Figure 14. Baseline Decision-Support Profile (Local Policy)

After the initial baseline performance test was conducted, DSP was treated with a 25% noise. The original dataset's 625 samples including the desired responses were divided into their respective PPL categories that are RED, ORANGE, YELLOW, GREEN, and NORMAL. After that, each category was randomly sorted.

Once sorting as completed, 25% of the samples were selected for modification of up to 1-bit difference. For example, if a desired response was [01000], then the modified sample could assume a value of [10000] or [00100] with an equal chance. In this manner, all of the noisy samples were then added back into the original dataset. The noisy DSP was then trained and tested using the noisy training data as the validation test set. The results of the baseline treated with 25% noise shows 88.20% accuracy with a learning rate of 0.005 (Figure 15). As the learning increases towards 1.0, the accuracy levels off at 91.81% with a learning rate of 0.3. A slight decrease from 91.81% to 91.60% is noticed when the learning rate is set to 1.0 (Figure 15). The MSE increased from 68.55 to 108.38, a 158% increase in the MSE from the baseline without noise. The baseline+Noise treatment decreased in accuracy and increased the MSE for the single baseline DSP. The average pass rate was 90.9% while the average MSE over the four learning rates was 78.8 over the previous baseline DSP MSE of 29.5.

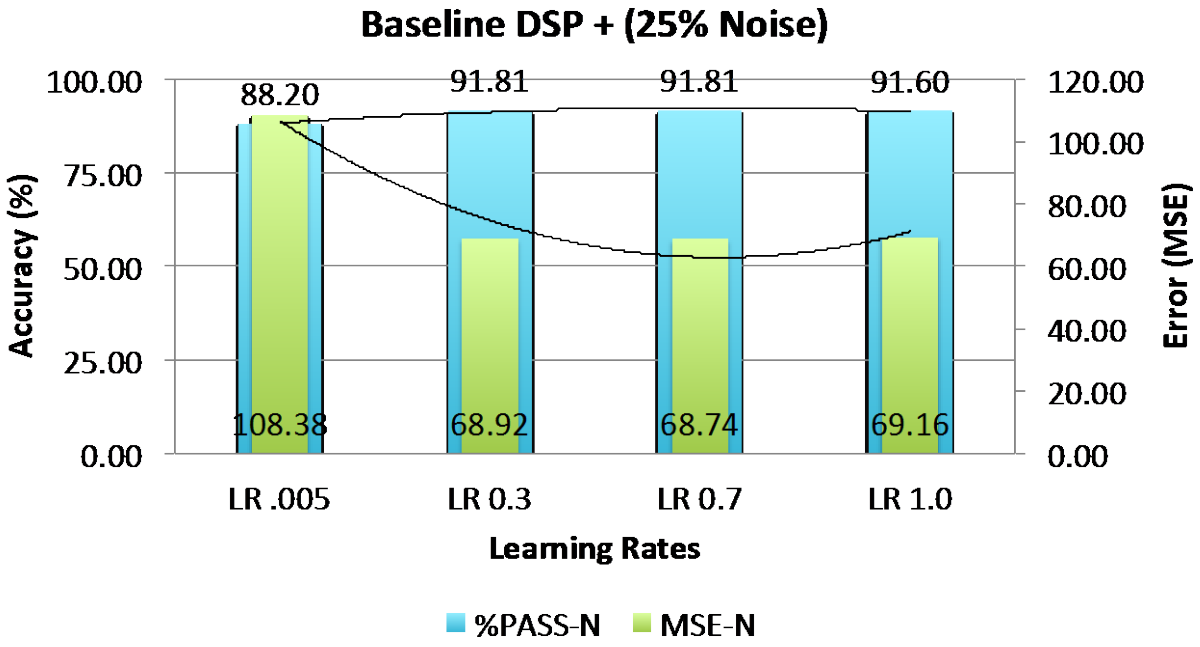

Figure 15. Single Decision-Support Profile Baseline +Noise Results

The purpose of the 9-fold cross-validation is to increase the generalization accuracy of the model. Figure 16 shows the performance results of the additional treatment of validating the baseline using 9-fold cross validation. The accuracy leveled out to 92.19% using a learning rate of 0.3. The error declined in a similar fashion as the baseline performance statistics. The test contained 105 samples that the ANN had never *seen*. This means that the model has an average generalization accuracy of 90.14% for unseen data using the same underlying threat distribution (i.e. Threat-severity level interpretations of KDD99 threat labels) despite the noise within the DSP's desired responses. This implies that the ANN can overcome some errors and can provide PPL recommendations 92.19% of the time for situation event patterns that was not included during off-line training. The 92% generalization accuracy of Lightning provides a method to approximate a desired response when faced with uncertain threat conditions for network defense.

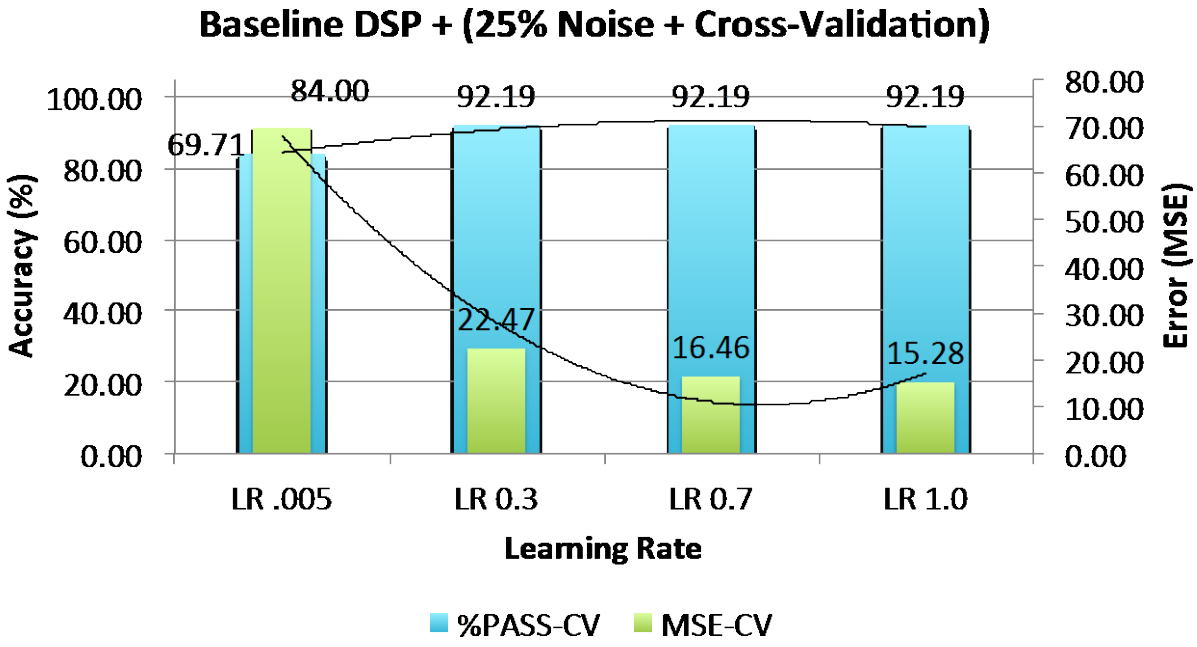

Figure 16. Single Decision-Support Profile Baseline +Noise+ CV Results

After the performance results were obtained for the baseline dataset and the two treatments, a side-by-side comparison of their results were made. All performance trends increase as the LR increases and the error generally decreases with the increased learning rate (Figure 17). The baseline has the highest accuracy of 98.02%, but may suffer against unseen events due to over fitting. The cross-validation treatment of the noisy baseline dataset had a lower MSE than the noisy dataset treatment validation method. The CV outperformed the baseline+noise, and provided a slightly higher generalization accuracy of 92.19%, which protects against over fitting when faced with unseen events. CV treatment significantly reduces the MSE of the baseline+noise dataset and performs closer to the baseline values (Figure 18).

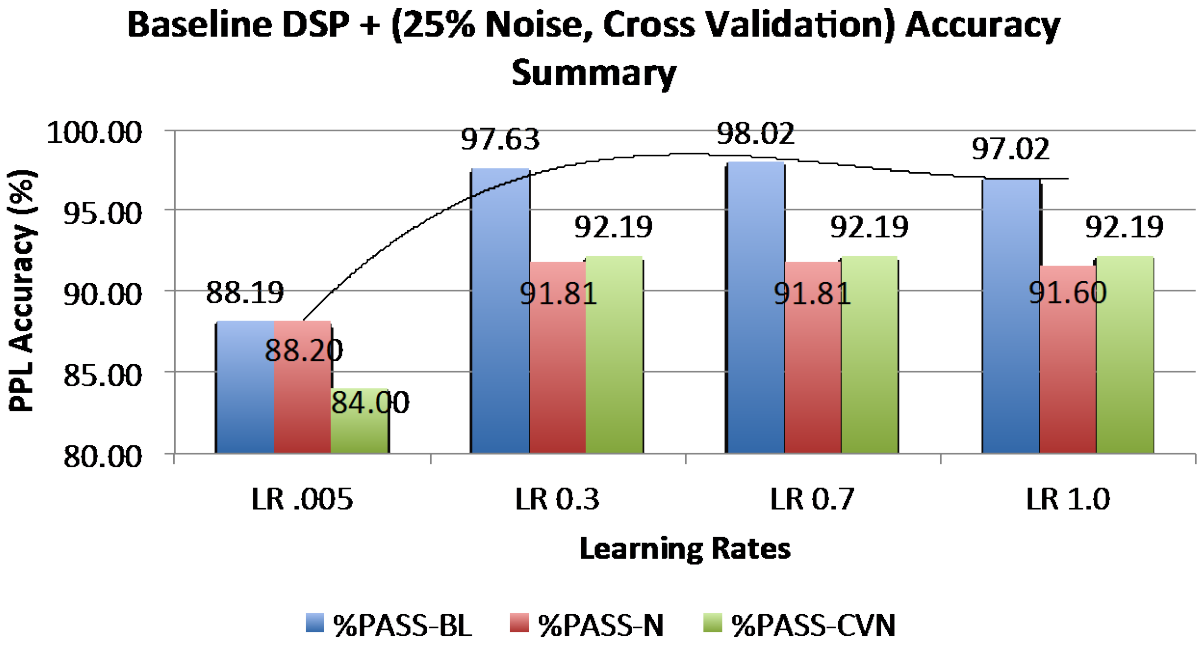

Figure 17. Single Decision-Support Profile Accuracy Summary Results

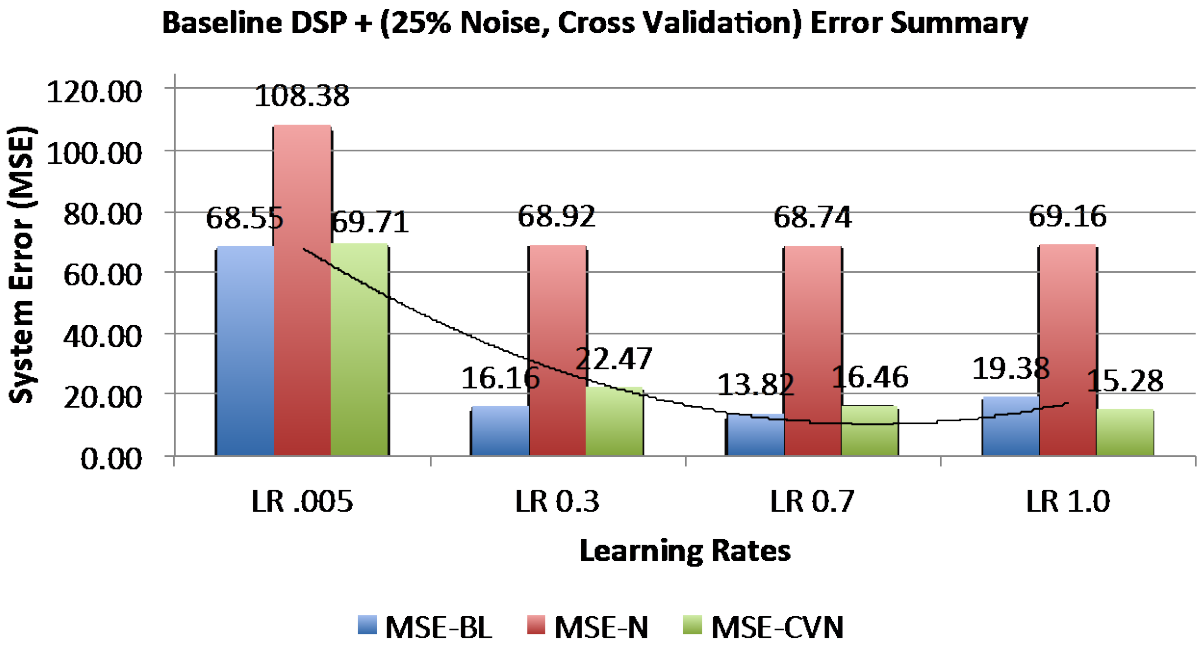

Figure 18. Single Decision-Support Profile Error Summary Results

In summary the results scenario II used the initial DSP performance values as the scenario baseline model. The affects of two progressive treatments, 25% noise and 9-fold cross-validation was evaluated. The DSP profiles for the baseline and the CV methods show an impressive PASS rate for Lightning. Using only a single DSP we can see that the threat distribution is favored for Area-A and the system MSE is representative of Area-A's localized interpretations of the global event. The data generally shows that as the learning rate increases, the performance rate increases but begins to level off after a learning rate of 0.7. A slight decrease on performance is shown when a learning rate of 1.0 is used.

The baseline average performance of 96.48% PASS is higher than the 90.14% cross-validation method and the average 90.9% accuracy level of the noisy treatment. This can be explained due to the increased errors that are associated with leaving a fold out or hidden from the ANN during training. Despite the generally higher MSE for the cross-validation rate, the model has a 92.19% generalization accuracy when recommending PPLs for events that it has never been trained on.

These findings are representative of a single participant's interpretation of a globally occurring event using Threat-Severity Level interpretations of the 10% KDD99 dataset. Finally in this section, we focused on a single DSP's interpretation of the threat distribution using reports from four neighbors. In the next section, we assess the performance of the ANN using multiple independent DSP s using their local policy strategy to interpret the same 10% KDD99 threat distribution.

4.3 Scenario-III Multiple DSP Interactions Results and Interpretations

In Scenario III we establish a baseline performance using the 625-sample distribution of the KDD99 dataset that has been interpreted into all combinations of the five Threat-Severity levels. Each Local area has submitted their DSP and overall strategy for interpreting the event distribution the 625 samples. The scenario validates the dataset with the training set and then uses 9-fold cross-validation. Each participant's accuracy increases as the error decreases using increased learning rates as seen in the single DSP baseline results (Figure 19). A special note highlights that the Baseline metrics are the same as the Single DSP baseline. Notice that the increases are slightly different, yet similar. The underlying common threat distribution may account for some of this. The other factor is the local DSP that makes a strategy based on what the event means to them. The local strategy is to win, and right now, the high roller has the accuracy.

The group baseline dataset achieves a modest 85.00% accuracy rate using a low learning rate of 0.005 (Figure 19). The low learning rates are good to provide the lowest error surface reduction in the hypothesis space where the desired local response matches the ANN's observed recommended PPL. However, lower learning rates takes longer to train the ANN's structure. As the learning rate increases for the system, the success rate level out at approximately 96.7%. The error is significantly reduced using a learning rate of 0.3 with this dataset set. There is no significant change when adjusting the LR to 0.7.

The same general performance is observed from a LR of 0.3. Very little difference was observed between a learning rate of 0.7 and 1. A learning rate of 1.0 resulted in an overall insignificant decrease in PASS success performance for the ANN from 96.89% using a LR of 0.007 to a PASS rating of 96.62%.

The primary cause of the highest MSE, shown in Figure 19 are related to the DSP constraints and inconsistent desired PPL responses when faced with tie-breakers found in Area-D's DSP Majority strategy, where interestingly, order appears to be learned by the ANN to consider and maintain local constraints imposed by Baseline's DSP. The error went down slightly from a system average of 15.58 to an average of 14 using a LR of 1.0. Area-C's Local-Only DSP strategy has the lowest local error because of the nature of its DSP, which is to recommend the local report only. Using this strategy, Area-C is an active reporter, but only listens to local reports. This strategy may be beneficial in some circumstances for the areas using a similar strategy.

The reporting nature of Area-C still provides the global event from which the global policy is derived. The fact that Area-C is reporting emphasizes the law of large numbers that effectively reduces the MSE for the ANN. The Baseline (Area-A) has the second highest rate of error still due to the constraints imposed by the local DSP. Finally, Area-D's majority DSP strategy remains high in local errors, while maintaining a 94% success rate. A summary of the baseline performance for group DSP's performance using the four learning rates provided in the next section. Area-A and Area-B benefit most from a learning rate of 0.7, while Area-C and Area-D show minimal increase in accuracy performance. Participants who choose to only provide threat reports also provide value to the other participants enabling a more accurate picture of a global threat occurrence. Area-C is a reporter only and desires a local reported PPL response only. Area-C's reports contribute to the Area-C had a slightly higher performance rating of 96.00% than the error prone Area-D which had the lowest averaging performance rating high of 94.00%.

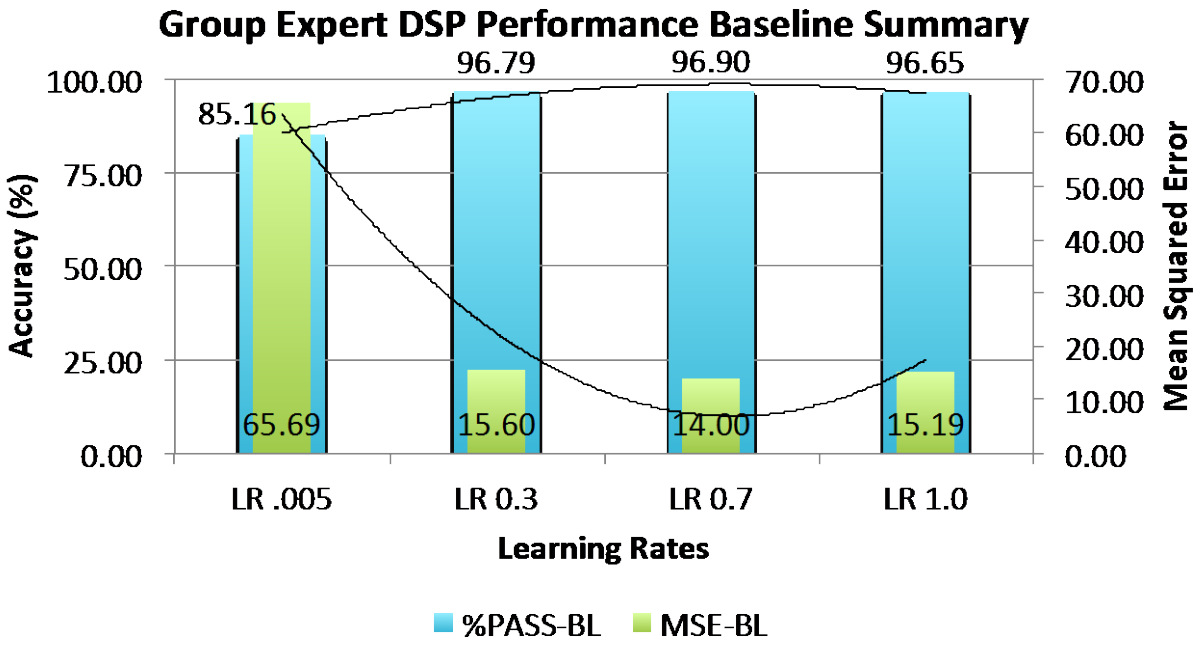

Figure 19. Group Decision-Support Profile Baseline Results

Figure 24 shows Area-B's *high-roller* DSP strategy has the highest PASS rate of 92.10% and the second lowest error of 57.7 using a low ANN learning rate of 0.005. Area-B's strategy desires the PPL recommendation to best mitigate or avoid the highest occurring global reported threat incident within the global event. Since this desired PPL recommendation is relatively consistent despite the order of *who* is reporting the errors are low. This means that the ANN is capable of determining when to consider threat order. Interestingly, when Area-B has a tie-breaking event, the ANN decides the tie-breaker instead of the local decision-maker as found with Area-D's *majority* DSP strategy, which results in a lower localized error. This implies that a local user should allow the ANN to choose the tie-breaking situation for majority vote strategies to minimize error and increase decision-support accuracy.

Area-D's DSP strategy that includes a random tie-breaker, it has the highest contribution of system error of 84.4 as shown in Figure 25. Contrasting Area-D's DSP strategy with The Baseline's DSP has a constraint that precludes the ANN from providing a "RED" alert unless it is from Area-A, the ANN considers the ordering of "who" is reporting within the training sample events. As a result, area A has the third highest local error among all participants. Area-C and Are-D's PASS% performance ratings are both approximately 80.20%.

Area-D has the highest error because its DSP strategy incurs a random tie break procedure when identical locally determined threat reports meet the same locally defined threat-severity level from the KDD99 threat distribution of report labels. Since the tie break consists one of the threats, and not a standardized choice, this induces localized error which makes the ANN's local MSE for the Majority DSP strategy increase from inconsistencies of decisions on the same set of events when order is not considered. It is noted that the ANN is capable of learning Area-D's strategy type, but needs more training samples to reduce the errors associated with the PPL recommendations. Area-C has the lowest error due to its DSP strategy to only desire PPL recommendation from its local IDPS. In the next section, we assess the generalization accuracy of the ANN using 9-fold cross-validation on the group-baseline, and testing with fold-9 as the hidden sample dataset.

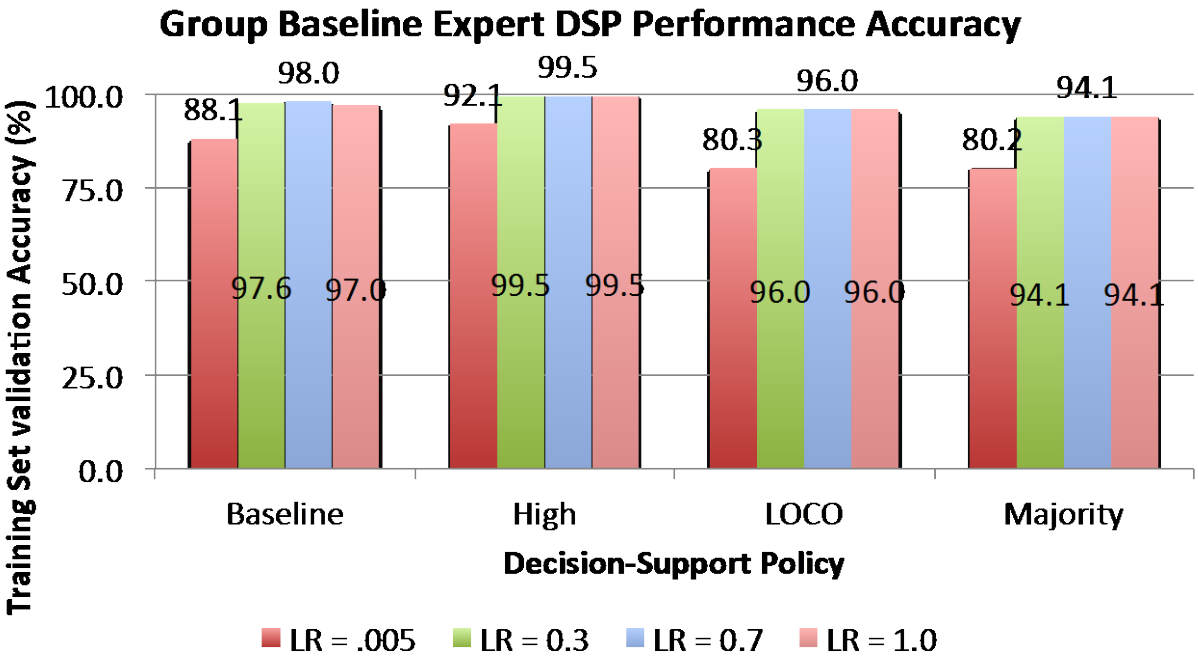

Figure 20. Group Decision-Support Profile Baseline PPL Accuracy Results

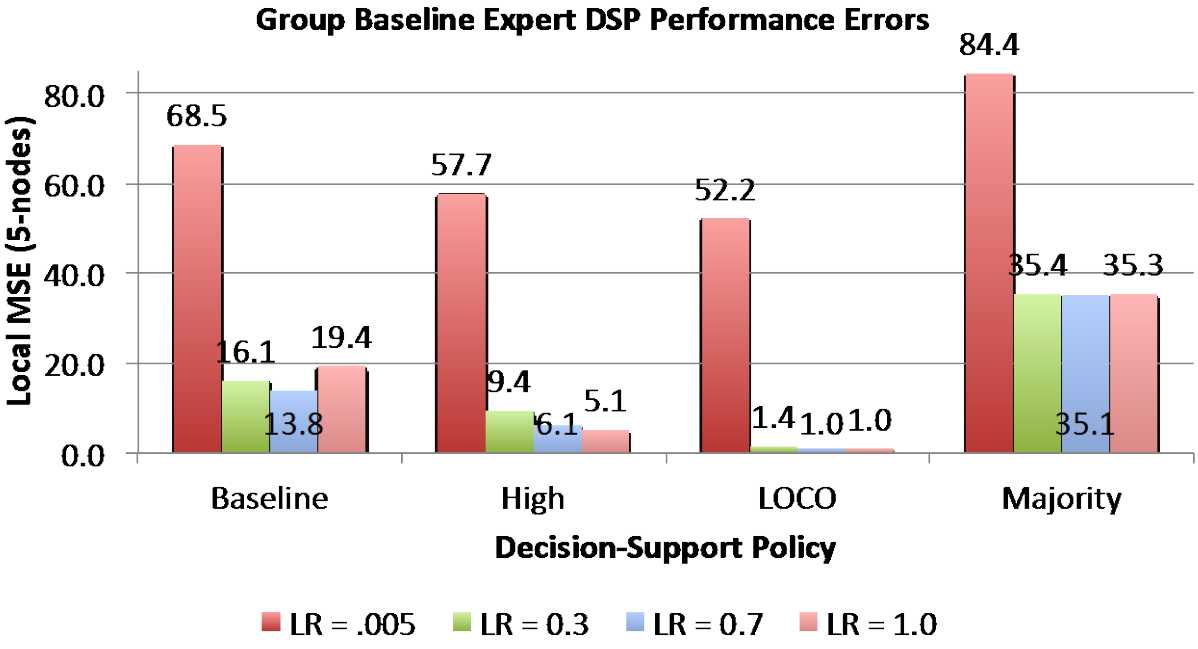

Figure 21. Group Decision-Support Profile Baseline Error Summary Results

4.4 Scenario-III Group DSP Baseline+CV Results and interpretations

We use cross-validation as before to obtain the generalization accuracy of the model. Similar results for the group DSP model using cross-validation are found when using a low learning rate for single DSPs. The system summary results are shown in Figure 23. The DSP performance accuracy is shown in Figure 24 and the Group DSP error is shown in Figure 24. The global average distribution of performance accuracy and error reduction performs similarity as the previous scenarios did. The global summary is representative of the individual DSP parts, but does not completely describe any single DSP.

The System performance rating continues to go up as the error goes down (Figure 22) as the performance tests progress through the learning rate levels. The Baseline DSP and Area-B had the highest error in the previous LR setting of 0.3. Using a 0.7 LR, The Baseline and Area-B increase their accuracy from 95.30% and 96.50% to 96.8% and 96.8% respectively. Area-C had no change in the accuracy rate while Area-D improved by half a percentage point. There is no significant difference in the performance results between a learning rate of 0.7 and 1.0. The errors went down for each area except for Area-D (Figure 24), which is explained by the tie-breaking DSP that generates inconsistencies. Interestingly, such inconsistencies produce similar behavior observed during the pilot study, where errors were found in the DSP desired responses.

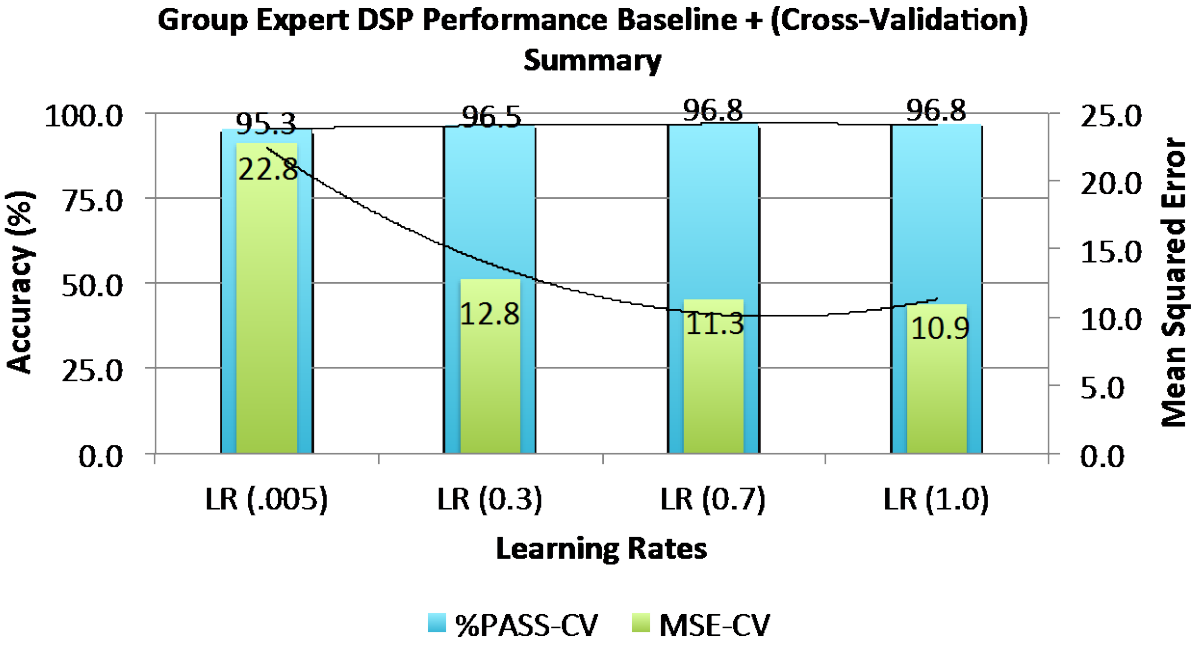

Figure 22. Group Decision-Support Profile Baseline+CV Results

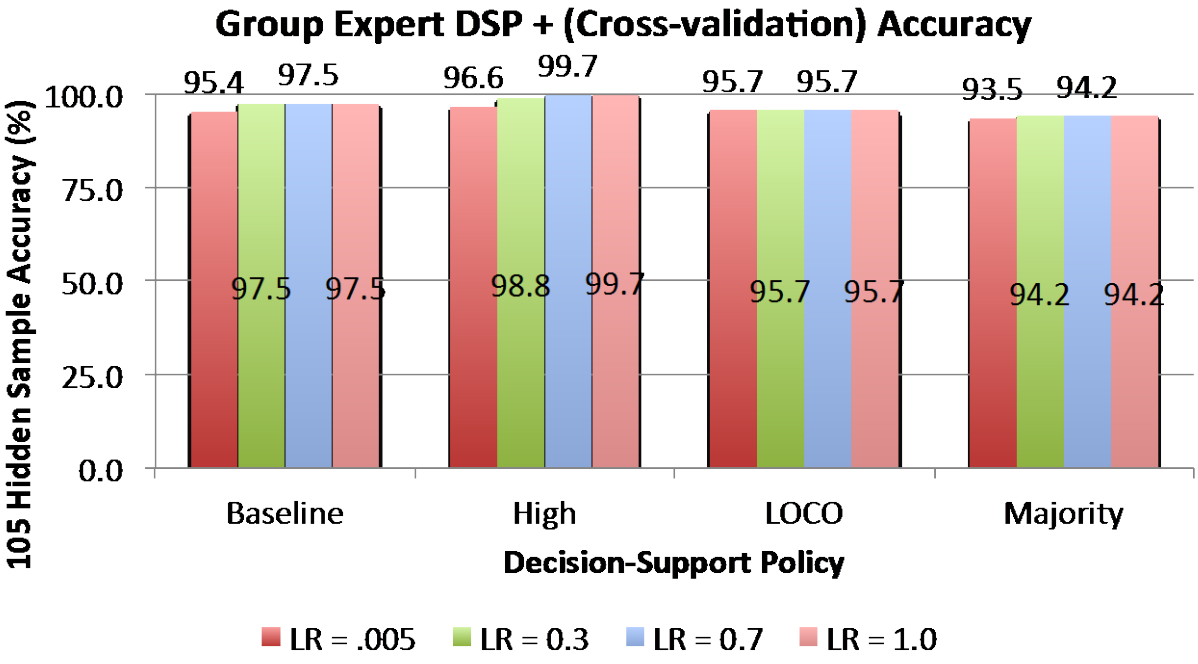

Figure 23. Group Decision-Support Profile Baseline+CV Accuracy Results

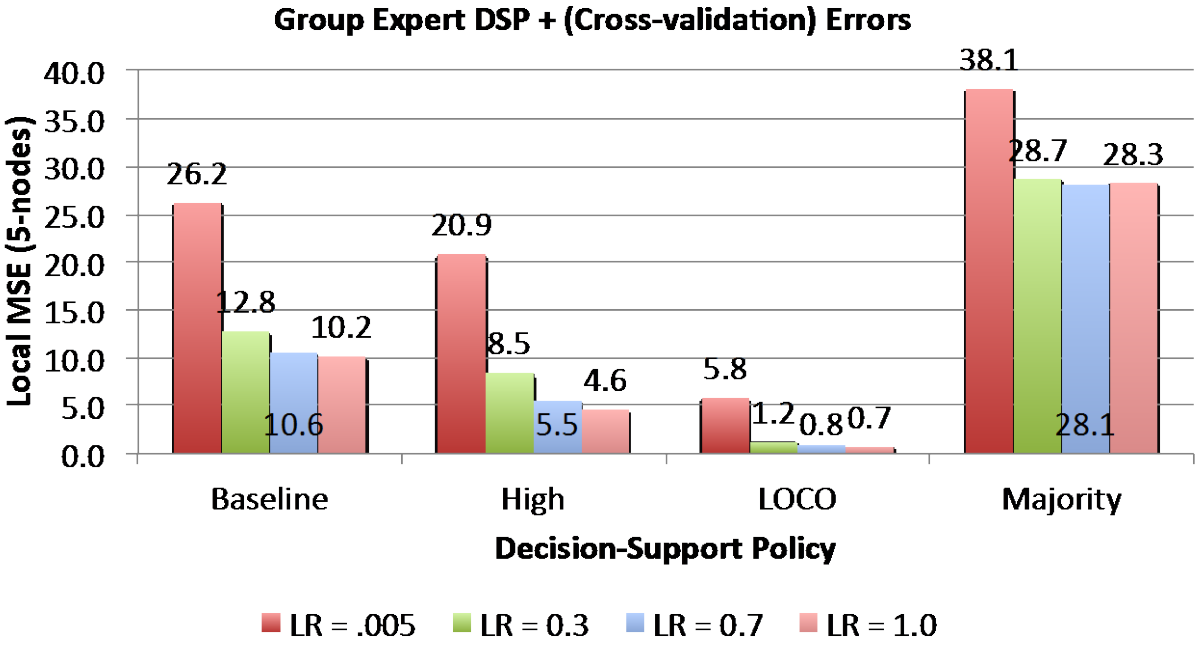

Figure 24. Group Decision-Support Profile Baseline+CV Error Results

4.5 Chapter Summary

In this chapter, the results of the pilot study, scenario I, and scenario II were presented. The modeling and simulations environment was successfully established using NetLogo to conduct the performance tests for the research. In addition, the data shows that arbitrary DSP m-of-n strategies can be learned independently using the same dataset distribution. The pilot study performance accuracy was 90.14%, with a MSE of 3.03.

In the second scenario of testing, the dataset distribution was increased to 625 samples using the Threat-Severity level mapping of the 10% KDD99 threat label distribution. The DSP strategy included a constraint to not recommend a PPL of RED unless the local area's IDPS detected a Type-I priority threat. This is significant, because the ANN learned this constraint despite an increase in errors with a low learning rate of 0.005.

With higher learning rates, the ANN achieved a 98.02% accuracy level and relatively low error of 13.82. The model performed well against a 25% noise treatment, but showed a high 1580% increase in the MSE with a low learning rate. At higher learning rates, the noise treatment achieved a 91.19% accuracy level. Using 9-fold cross validation, the ANN's accuracy improved significantly over the noise treatment, and achieved a generalization accuracy of 92.19 despite a 25% noise treatment using cross validation. Additionally, employing the 9-fold cross-validation method significantly reduced the MSE, bringing the average MSE near baseline values.

The Group cross-validation performance results show that the individual DSP desired responses are independent of the other participant's responses for local performance and local error statistics where Area-A's baseline DSP performance metrics were statistically the same when comparing the single DSP results in scenario –II to the group DSP results in scenario III. Using a single set of output nodes for Area-A's DSP, we saw an average performance accuracy of 97.00% without cross-validation and a generalization accuracy up to 92.10% using cross-validation against a 25% noisy DSP dataset. The Majority voter DSP experienced the highest local error, but the other areas were not affected.

Finally, the data shows that lower learning rates show the lowest accuracy using the parameter settings and the highest error. This is expected and during the pilot studies, the lower learning rates are commonly used for longer running times (Mitchell, 1997). The moderate learning rates of 0.3 and 0.7 had mixed results and appear to level off after a learning rate of 0.3 is used. Learning rates above 0.7 did not realize significant increases in performance for the system and maintained an average PASS% rating of 96.8%.

V. Conclusions and Recommendations

This Chapter provides the conclusion of the research effort, significance, recommended actions and recommendations for future research. If situation awareness is to be enhanced, the critical elements of the operational environment must provide interesting meaning beyond a localized environment for other participants to join ANN-based network structure. Aggregating the reports of multiple independent participants in real-time provides a common distribution of globally occurring events that may lead to a normalized distribution of reported events given enough numbers. With enough participants that provide accurate real-time reports about their locally occurring threats, a strength-in-numbers approach to global network defense can emerge. The emergent behavior of such reporting and aggregation of global events can then be learned by the ANN-based model and provide localized decision-support to otherwise isolated network security boundary defenders in Cyberspace.

Emergence is a phenomenon where aggregate behavior arises from localized behaviors Miller and Page (2007). This research modeled individual LANs as agents that are interconnected using a single layer feed forward ANN. The LANs are modeled as independent heterogeneous entities with localized threat mitigation and avoidance behaviors. The goal of aggregating the micro behaviors of local IDP LANs, was to develop a process to enable a common understanding of a more global or macro behavior. As a result of this goal, the macro behavior can be developed into a global policy response that the ANN can learn.

The seemingly random occurrence of local threats becomes an aggregate common variable or global event learned by the ANN. The global event enables situation awareness for previously unaware local decision-makers. This implies that the micro behavior of localized LAN reporting results in a diverse set of macro behavioral global response actions.

The aggregated actions learned by the ANN using the DSP and Off-Line training components produces the capability to detect the occurrence of global threat event patterns from previously unaware threat distribution occurrences. The ANN learns to detect and recommend PPLs to localized network defenders based on expert DSPs. As more and more LANs participate, according to the Central limit Theorem (Miller and Page 2007) and the law of large numbers (Renze & Weisstein, 2014), a normal distribution of global policies may emerge. This assumes that the threats are the common distribution that underlies this entire collaborative process.

This claim is debatable because the claim of emergent behavior is artificially induced emergent behavior and we can attribute the direct cause. Natural emergent behaviors are not strictly *non-deterministic* in nature (Mitchell, 1997). In addition, decision-support systems (DSS) should be carefully considered when employing in dynamic environments especially when the meaning of a critical element cue status has changed and the DSS has not.

5.1 Significance and Contributions of Research

By encoding expert decision-support profiles with an ANN-based structure, a 99.7% accuracy recommendation can be made to novice network security professionals in Cyberspace. This recommendation has the potential to provide actionable threat mitigation and avoidance measures that could minimize threat risk. Research should continue with more advanced ANN concepts that are promising in the support of localized decision-support recommender systems in Cyberspace.

The research effort makes three contributions. First, the research provides results that warrant continued research in ANN-based DSSs for localized decision-making in Cyberspace. Secondly, the decision-support profile survey is provided in the hopes that it may be useful in future DSP development.

Finally, the modeling and simulations environment tool can be used across multiple disciplines to integrate concepts of network engineering and artificial neural networking. This modeling and simulations tool has the additional capability of being extended across a local area network using the GitHUB capability. This extended capability along with the existing tool can enhance understanding about complex adaptive systems, to include intrusion detection and prevention networks.

5.2 Recommendations for Action

This research makes three recommendations. (1) Pursue the development of collaboration of IDPS environments to share threat information as teams. Teams working together naturally have established Team SA element cues, and should be identified, modeled and validated as SA elements. Employ collaboration capability to enable mobile IDPS teams that need immediate reach back capability or simply need help in searching for an item of interest. Having other team members to share potentially, actionable information enhances the IDP's local defender. (2) Continue development of the modeling and simulations environment and focus on the following areas; (a) Establishing trusted collaboration membership pools, (b) Identify, model and simulate critical shared team SA requirements. The survey provides a way ahead for individual SA requirements that should be modeled, simulated and validated continuously. Shared or Team SA are those things that the team shares amongst the group that they need to know in order to make team-based decisions in real-time environments, (c) Employ secure cloud computing services to host mobile Cyber Teams in order to provide distributed threat situational awareness and parallel search of interesting item capabilities, (d) Incorporate well-established Hub, GitHub technology and develop secure communications platforms that are customizable for global teams. NetLogo support GitHub.

(3) Conduct a goals-directed task analysis for IA security and Cyber professionals that perform duties in the IDSP operational environment. A Delphi study should also be considered.

The survey attached in the Appendix A may provide an excellent start in determining newly developing individual and team SA critical elements. The decision-support profiles are the critical elements that are necessary to identify the critical SA requirements. Once identified, they must be incorporated into a simulations environment, validated and tested for effectiveness to keep pace with evolving trends.

The larger research effort should focus on advanced ANN concepts and structures for use in collaborative networking environments. Conduct research to find a way to secure local area expert decision-support profiles and group collaboration efforts. Conduct research efforts to establish universal ANN output nodes that can serve as worldwide listening posts for threats. Participants can subscribe to such an infrastructure.

5.3 Research Summary

Supporting the local defender has been the enduring and sustaining element for this research. Understanding the complexities of a CAS is a challenge in and of itself when going it alone. Isolated network defenders can enhance their local situation awareness and gain strength-in-numbers on Cyberspace's CAS operational battlefield. In Cyberspace, the need for w wide-area infrastructure of customizable and team supported DSSs is necessary. Artificial intelligence, using ANN technology to develop a universal or global threat event recommendation system is critical for today's isolated network defenders.

A call for developing a 'strength-in-numbers' approach to intrusion detection and prevention using artificial neural networks was made. This call is made in an effort to enhance the SA of the local decision maker by providing global awareness of interesting threat reports.

The problem of how best to model Cyberspace as a CAS was addressed in Chapter I to develop a context. The motivation for conducting this research effort is to always assist the local decision maker in a complex and adaptive world. Decision-making is hard, and chapter reminds us of how hard it is to develop DSSs like the IDPS. Chapter II provided a more detailed explanation of the evolution of the Intrusion detection process, the properties of complex adaptive systems to include non-deterministic emergent behavior.

The literature review discussed situation awareness, decision-support systems, emergent behavior, and the role of artificial intelligence in decision-support systems, specifically in the intrusion detection process. A discussion of artificial neural networks focused on machine learning led us to better understand feed forward ANNs. The back propagation algorithm was introduced to understand how the ANN reduces the error surface in the hypothesis space to form the global policy link structure and provide best-fit protective posture recommendations to novice defenders in uncertain situations using learned expert recommendations after considering the threat event risk factor.

The capability to reduce the error surface is enabled by gradient descent and the delta rule to provide stochastic approximations of unseen patterns. Using the sigmoid activation increased the understanding and capability of ANNs. The modeling and simulations environment as the system under Test was introduced in Chapter II consisting of the local Decision-Support and Off-Line critical components under test. Lightning was introduced and the global policy reporting recommendation output was revealed at the end of Chapter III.

The results of adjusting the learning rate of the ANN with 0.005, 0.3, 0.7 and 1.0 values show that the ANN can accurately recommend the learned protective posture levels of expert decision-makers 90% of the time using a noisy decision-support profile and 9-fold cross-validation.

Without cross-validation or noise the ANN has a recommendation accuracy of 99.7% for the baseline profile. When tested using four independent decision-support profiles in collaboration, the ANN's average generalization accuracy improves to 96.35% without noisy decision-support profiles and 9-fold cross-validation. The research shows potential for group collaboration using ANN-based decision-support systems, which can support a strength-in numbers approach to network defense.

Appendix A Decision-Support Profile Survey

Determining Decision-Support Profiles in Collaborative Event Detection Environments

Pre-Artificial Neural Network Encoding Survey: Investigator's Interview/Admin questions.

MAJ Brian G. Woolley, PhD, Primary Investigator

MAJ Tyrone A. Lewis, Master's Student

7/10/2014

This is a four part anonymous study to determine the effects of event collaboration on human decision-support profiles. When faced with two network threat scenarios, respondents are expected to recommend a protective posture that best protects their local-area network security boundary. During Part 1 (Respondent Background), the respondents are asked to provide their closest matching IA work role and are introduced to the concepts and materials used during the study. In Part II (Isolated Threat Mitigation Model Scenario-I) the respondents are asked to respond to the available threat reports while isolated from threat collaboration with other outside sources. The event sequence is repeated in Part III (Collaboration Threat Mitigation Model, Scenario-II); however the respondents are now authorized to collaborate and interpret credible/participating neighbor's reports from a wider-area about their threat event's occurrence. Finally, in Part IV (Participant Reflection) questions are asked to determine if there was a decision-support profile change. Following the closing of the survey, respondents are asked to participate in an after action review.

(The investigator should print this packet out and read the script while conducting the survey)

Questionnaire and Quick Reference List- (For Administrative Use)

1. **Respondent Background Questionnaire (11 Questions)**
   Figures/Tables Used: Response Sheet
   References Available: None
2. **Understanding the Threat Questionnaire (Part-Ib) (23 questions)**
   Figures/Tables Used: Response Sheet (Table 1.)
   References Available: Instructions and rating scale
3. **Scenario-I Questionnaire (Part-II Isolated) (30 questions)**
   Figures/Tables Used:
   - Response Sheet

   References Available:
   - Scenario-I Threat Brief Summary
   - Figure 1. *Intrusion detection alert and response matrix*
   - Figure 2. *KDD99-apwxific categorized threat label definitions*
   - Figure 3. *Resource Protection List for Area-A*
   - Figure 4. *Isolated Threat Mitigation Model* (Network Diagram)
4. **Scenario-II Questionnaire (Part-III Collaboration) (30 questions)**
   Figures/Tables Used:
   - Response Sheet

   References Available:
   - Scenario-II Threat Brief Summary
   - Figure 1. *Intrusion detection alert and response matrix*
   - Figure 2. *KDD99-apwxific categorized threat label definitions*
   - Figure 5. *Neighbor Resource Protection List for Area-A*
   - Figure 6. *Collaborative Threat Mitigation Model* (Network Diagram)
5. **Reflection Questionnaire (9 questions)**
   Figures/Tables Used: Response Sheet
   References: None
6. **After Action Review (5 questions)**
   Figures/Tables Used: Response Sheet
   References: None

Survey Script

Pre-Survey

Reserve an appropriate room. Locate Bathrooms, Emergency exits, Rally Points

Place Pencil, scratch paper and respondent IDs on desk/survey stations.

Prepare and print survey packets that should include the following materials;

- Respondent/Survey ID
- Individual Respondent Reference Materials
- Background Questions
- Self-Assessment KSA questions
- Threat Understanding Questions
- Scenario-I questions
- Scenario-II questions
- Reflection Questions
- Scratch Paper

Open Survey Session:

AINV: Good morning/afternoon, Welcome to this research survey session. I am MAJ Tyrone Lewis and I will be administering this survey today. Before we begin, I have a few administrative announcements:

Administrative Announcements:

Indicate the location of bathrooms, emergency exits, etc… Issue prepared survey materials to respondents:

READ PRIVACY: (Privacy Act Statement obtained from human Subjects POC). Personally, Identifiable Information will not be collected in this survey. The survey is anonymous so please do not mark any specific duty location, or PII that could be used to specifically identify you as an individual.

READ CLASSIFICATION: This survey is UNCLASSIFIED. You should not discuss, disclose or indicate anything that has a classification marking higher than UNCLASSIFIED. At the end of the survey, please review any responses to ensure that you have not disclosed any intentional or unintentional CLASSIFIED information.

READ USE OF DATA: Data will be used to support graduate level research.

AINV: Are there any questions so far?

(Administratively answer respondent's questions before proceeding to the next section)

AINV: If there are no further questions, we will proceed with the survey. This survey consists of four parts.

AINV: You are about to take Part-Ia, Respondent background questions.

READ PURPOSE: The purpose of the background questions section is to evaluate and assess your general background with threat mitigation, risk management, and network security experience.

READ DIRECTIONS: Please indicate the work role that best represents you the most at the top of the questionnaire. On the top right corner of the questionnaire, please write in your respondent ID. You will be presented with 8 multiple choice questions, 2 priority ranking questions and 1 short answer response to add optional comments. You should carefully read each question and all of the available choices before making your final selection. If a choice does not specifically address your background, you should select the choice that best reflects your general background and experience. You may use scratch paper to add additional information if you would like.

Explanation of Terms: IDS, IDPS, PAN, LAN, WAN, Cisco, Juniper, DoD 8570.1M, Physical mediums, OSI Layer 1 technologies, local policy, global policy, watch-list, active threat, threat types and protocols.

REFERENCES: You may use the attached definitions if necessary.

AINV: After you have completed the questionnaire and are satisfied with your choice selection, please hand the questionnaire to me.

ASK: What questions do you have so far?

(Administratively answer respondent's questions)

Issue questionnaire to respondents

AINV: You may now begin:

(After all questionnaires have been turned in, close the session)

AINV: We will now proceed with Part-Ib (Threat Understanding Questions)

AINV: You are about to take Part-Ib, "Understanding the Threat" questionnaire.

READ PURPOSE: The purpose of the "Understanding the Threat Questions" is to see how familiar you are with specific network threats and malicious traffic signature labeling methods. This survey derives the label names and threat descriptions from the KDD99 dataset. The KDD99 dataset is a database containing a standard set of data to be audited, which includes a wide variety of intrusions simulated in a military network environment [KDDCUP99].

HAND OUT rating scales.

AINV: You should have two pieces of paper for this questionnaire. The first sheet describes the response categories, while the second sheet is the table used for recording your responses.

READ DIRECTIONS: Please turn your attention to Table 1. Please take note that the table is partitioned into three parts. In the center of the table, the merged column heading (KDD99's Threat Classification labels) lists each threat that appears in the KDD99 dataset. On the Left hand-hand side of Table-1 you will see five smaller columns. This is where you will rate your previous and current knowledge of the threat for each threat label. On the right hand side of Table-1, is where you will record the perceived level of the threat as indicated in the center column for that particular row.

REFERENCES: KDDCUP99, https://archive.ics.uci.edu/ml/machine-learning-databases/kddcup99-mld/kddcup99.html, last accessed July, 13 2014.

AINV: After you have completed the questionnaire and are satisfied with your choice selection, please hand the questionnaire to me.

ASK: What questions do you have?

(Administratively answer respondent's questions)

AINV: You may begin:

(After all questionnaires have been turned in, close Part-Ib)

AINV: Thank you for your participation in Part-Ib.

Return from Break

AINV: You are about to begin Part-II of the survey. You will receive a Scenario Threat briefing that may be used as a reference to complete the follow-on questionnaire. After

the threat brief is given, you will be presented with two example questions. After the threat brief and example questions are given, you will have the opportunity to ask questions before beginning the section questions.

READ PURPOSE: The purpose of Questions set 1a is to evaluate your decision-support preferences when responding to threat information based on defined local policy, organizational goals and your interpretation of the threat that may occur in your local network security boundary.

Conduct Threat Briefing (~10 minutes)

HAND OUT Scenario-I package.

READ DIRECTIONS: (Read the threat brief.)

Describe References: Figure X.

Read example question one and example two question two.

AINV: After you have completed the questionnaire and feel satisfied with your choices, please hand the questionnaire to me.

ASK: What questions do you have?

(Administratively answer respondent's questions)

Scenario-I questions

READ INSTRUCTIONS: Recommend the appropriate protective posture for each round in the table below by circling the recommendation that best mitigates the threat. You should only select one choice per question. You are free to use scratch paper while taking this survey, but they must be turned in to the investigator at the end of the survey. Please clearly circle one and only one letter per response row.

R = RED, O = ORANGE, Y = YELLOW and G = GREEN (See reference Figures 1, 2 and 3 if necessary)

You may now begin:

(After all questionnaires have been turned in, close Part-II)

AINV: You are about to begin Part-III of the survey. You will receive a Scenario Threat briefing that may be used as a reference to complete the follow-on questionnaire. After the threat brief is given, you will be presented with two example questions. After the threat brief and example questions are given, you will have the opportunity to ask questions before beginning the section questions.

READ PURPOSE: The purpose of Questions set 1b is to evaluate your decision-support preferences when responding to threat information based on defined local policy, organizational goals and your interpretation of the threat that may occur in your local network security boundary.

Conduct Threat Briefing (~10 minutes)

HAND OUT Scenario-I package.

READ DIRECTIONS: (Read the threat brief.)

Describe References: Figure X.

Read example question one and example two question two.

AINV: After you have completed the questionnaire and feel satisfied with your choices, please hand the questionnaire to me.

ASK: What questions do you have?

(Administratively answer respondent's questions)

Scenario-II questions

READ INSTRUCTIONS: Recommend the appropriate protective posture for each round in the table below by circling the recommendation that best mitigates the threat. You should only select one choice per question. You are free to use scratch paper while taking this survey, but they must be turned in to the investigator at the end of the survey. Please clearly circle one and only one letter per response row.

R = RED, O = ORANGE, Y = YELLOW and G = GREEN (See reference Figures 1, 2 and 3 if necessary)

You may now begin:

(After all questionnaires have been turned in, close Part-III)

AINV: You are about to take Part-IV, Reflection Questions

HAND OUT rating scales.

AINV: This questionnaire has four questions.

READ DIRECTIONS: You are about to take Part-IV "Reflection Questions"

The purpose of the reflection questions:

READ PURPOSE The purpose of the reflection questions is to allow you to provide insight into how you felt when making your protective posture decisions for scenarios I and II questionnaires.

You will be presented with nine multiple choice questions. You should carefully read each question and all of the available choices. After you have read the question and choices, briefly recall the scenarios that you just completed where neighbor collaboration was considered or not. Choose the best answer that most closely matches your response.

You may use scratch paper to add additional information if you would like.

(Discussion: The reflections questions are designed to see if the security professional's responses changed after they became aware of additional threat information. Often times, the decision-making process is not completed until after someone has had the opportunity to reflect on the decisions that they have made. In some instances, positive reinforcement encourages the decision-maker to make the same decision under similar circumstances. A less confident decision-maker may choose an alternate choice if they did not obtain positive feedback after making an uncertain choice (Endsley & Garland, 2000).

REFERENCES: None.

AINV: After you have completed the questionnaire and are satisfied with your choice selection, please hand the questionnaire to me.

ASK: What questions do you have?

(Administratively answer respondent's questions)

AINV: You may now begin:

(After all questionnaires have been turned in, close Part-IV)

Close Formal Survey. (Collect all materials and given respondents the opportunity to screen response sheets for classification or PII violations. DO NOT ALLOW RESPONSES TO BE CHANGED.)

Conduct AAR (optional)

AINV: The formal portion of this survey has been completed and you are free to leave. Before you leave, please ensure that you have all of your personal belongings, that you have not provided any classified information to this survey and that you have turned in all of your scratch paper that has your respondent ID clearly indicated in the top right hand corner. For those who have the time to stay, please help us improve this survey by providing valuable feedback.

ASK: Would you like to participate in this feedback?

AINV: We will next conduct an after action review session.

ASK: What went right?

RECORD:

ASK What went wrong?

RECORD:

ASK: What was supposed to happen?

RECORD:

ASK: What was good or should be sustained in this survey?

RECORD:

ASK: What was bad/unclear or should otherwise be improved to make this survey better?

RECORD:

ASK: What else would you like to add to this survey process?

RECORD:

AINV: On behalf of AFIT, Dr. Davis, MAJ Woolley and ENG, I would like to personally thank you for your participation in today's survey. My contact information is on the board if you would like more information about this survey or the ongoing research. Have a great day!

Respondent Survey Package

Pre-Artificial Neural Network Encoding Survey: Investigator's Interview/Admin questions.

MAJ Brian G. Woolley, PhD, Primary Investigator

MAJ Tyrone A. Lewis, Master's Student

7/10/2014

(Intentionally Left Blank)

PART Ia - Respondent Background Questions (1 of 3)

Work Role: _____ Respondent ID: _____

1. On average, how many hours did you work per week as an Information Assurance (IA) security professional?

- o Greater than 40 hours
- o Between 30-40 hours
- o Between 20-30 hours
- o Less than 20 hours

2. What types of Intrusion Detection/Prevention Systems (IDPS) have you managed, operated, administered or have technical knowledge of? (Circle all that apply)

- o Cisco ASA Models
- o Snort
- o Juniper
- o Next Generation IPS
- o Other IDPS, Firewalls, ACLs

3. As an IA security professional, how many hardware or software devices/packages have you protected within your network boundary using one or more IDPS devices.

o None	NA
o Less than 5	HW/SW
o 5 - 9	HW/ SW
o 10-99	HW/SW
o 100 - 999	HW/SW
o More than 1000	HW/SW

4. Select the largest sized communications network that you have personal experience with as an IA security professional.

- o Personal Area Network
- o Local Area Network
- o Campus Area Network
- o Metropolitan Area Network
- o Wide Area Network
- o Physical (Not network-based)

PART Ia - Respondent Background Questions (3 of 3)

11. Briefly describe additional comments here.

(Intentionally Left Blank)

Part Ib. Understanding the Threat Questions

Table 1 requires two responses for each attack classification signature label. The name of the attack is indicated in the center column. On left side of Table 1, rate your knowledge and experience level using the scale below (from 1 to 5):

- 1 = Advanced. I possess specialized knowledge and could instruct others on the principles of mitigation tactics techniques and procedures used to monitor, detect, respond and mitigate this attack.
- 2 = Intermediate. I am familiar with this attack classification and I have mitigated the attack classification frequently using Local Policy and best practice TTPs)
- 3 = Experienced (Can execute mitigation, avoidance or prevention TTPs IAW local policy.
- 4 = Beginner. I am unfamiliar with this attack, however I feel confident that I can use IDPS indicators and local policy response procedures to mitigate this attack with some supervision.
- 5 = No Experience. I have never mitigated, seen, and/or cannot define this attack.

Use the **right** side of Table 1 to indicate your perception of the attack's ability to threaten ongoing mission or organizational goals using a scale (from 1-4) [Cisco Best Practices]

- 1 = RED. **High** Impact or data that if compromised, would cause an extreme disruption in the business, cause major legal or financial ramifications, or threaten the health and safety of a person. The targeted system or data requires significant effort to restore or the restoration process is disruptive to the business or other systems.
- 2 = ORANGE.**Moderate** Impact (compromised systems/data viewed by unauthorized personnel, data corrupted, or data lost) disruption in the business, minor legal or financial ramifications, or provide further access to other systems. Moderate effort to restore or process is disruptive to the system.
- 3 = YELLOW **Low** Impacting threat events to systems within the network boundary or data that if compromised (data viewed by unauthorized personnel, data corrupted, or data lost) would not disrupt the business goals and objectives or cause legal or financial ramifications. System restoration is easy.
- 4 = GREEN **None**. No impact to business goals or objectives.

(Intentionally Left Blank)

Part Ib. Understanding the Threat Questions

Work Role: _____ Respondent ID: _____

Table 12. Individual's severity rating of KDD99 dataset's threat labels

Threat Experience Level					**KDD99's threat Classification Labels**	**Perceived Threat (Risk) Impact to Local Goal(s) accomplishment**			
1	**2**	**3**	**4**	**5**		**R(4)**	**O(3)**	**Y(2)**	**G(1)**
					back				
					buffer_overflow				
					ftp_write				
					guess_passwd				
					imap				
					ipsweep				
					land				
					loadmodule				
					multihop				
					neptune				
					nmap				
					normal				
					perl				
					phf				
					pod				
					portsweep				
					rootkit				
					satan				
					smurf				
					spy				
					teardrop				
					warezclient				
					warezmaster				

(Intentionally Left Blank)

PART-II Scenario-I [1a]
Scenario Threat Brief

Specific Situation: You are the IA security professional for Area-A's network security boundary. Various network security breaches are occurring in and around your locally defined area and throughout the wider-area's operational environment. Each PPL recommendation chosen is an independent response.

Your Role: You decide the overall protective posture level (PPL) that should be assumed by Area-A in order to protect and defend your mission-critical resources IAW local policy. You use threat reports and context clues to support your decision when recommending the best PPL for your local Area.

Your goal: Recommend a PPL that you believe well allocates your protection resources' ability to mitigate the occurring threat and minimizes the cost of adverse effects on normal operations.

Local policy: Priority threats have the highest consideration for PPL recommendations. You should choose the PPL (i.e. red, orange, yellow or green) that you feel is best to mitigate the reported threat for the near-term future. PPL recommendations should be executed immediately.

Global Policy: Neighbor collaboration **IS NOT** authorized.
You are aware that you have neighbors (Area-B, Area-C and Area-D, Area-F, Area-X) that may provide threat reports.

The following neighbor's threat reports about their protected resources are trustworthy:
NONE

Specific network vulnerabilities: These threats have a risk factor greater than or equal to 80% and have priority for threat mitigation within your security boundary;

Perl, rootkits, buffer_overflows, and **loadmodules** signatures.
(See Figure 1 and 2)

SUMMARY:

Monitor the status of your active threat '***watch-list***'

Detect the status of occurring threats as reported.

Respond appropriately to operational environment threats by recommending the best protective posture to meet local goals and objectives. Indicate your response by circling RED, ORANGE, YELLOW or GREEN.

References, Figures 1, 2, 4 and 4.

(Intentionally Left Blank)

Part II - Scenario-I
Example Questions and Discussion

Example Question 1.

	Credible IDPS Reports-a	Recommended Protective Posture			
Round	**Area-A**				
39	perl	**R**	**O**	**Y**	**G**

Discussion: Area A's IDPS is currently reporting/logging the detection of a *perl* threat. You consider all credible sources to include authorized neighbor reports, your own KSAs and policy guidance to make the best protective posture recommendation to mitigate the threat in the future.

	Credible IDPS Reports-a	Recommended Protective Posture			
Round	**Area-A**				
39	*perl*	**R**	**O**	**Y**	**G**

Clearly CIRCLE one PPL recommendation as R, O, Y or G.

Example Question 2.

	Credible IDPS Reports-a	Recommended Protective Posture			
Round	**Area-A**				
16	*smurf*	**R**	**O**	**Y**	**G**

Discussion: Area A's IDPS is currently reporting/logging the detection of a *smurf* threat. You consider all credible sources to include authorized neighbor reports, your own KSAs and policy guidance to make the best protective posture recommendation to mitigate the threat in the future.

	Credible IDPS Reports-a				
Round	**Area-A**	**Recommendation**			
16	*smurf*	**R**	**O**	**Y**	**G**

Clearly CIRCLE one PPL recommendation as R, O, Y or G.

(Intentionally Left Blank)

Part II - Scenario-I [A]
Start: _____ END: _____

Work Role: _____ Respondent ID: _____

Instructions: Recommend the appropriate protective posture for each round in the table below by circling the recommendation that best mitigates the threat. You should only select one choice per question. You are free to use scratch paper while taking this survey, but they must be turned in to the investigator at the end of the survey. Please clearly circle one and only one letter per response row.

R = RED, O = ORANGE, Y = YELLOW and G = GREEN (See reference Figures 1, 2 and 3 if necessary)

	Credible IDPS Reports-a	**Recommended Protective Posture**			
Round	**Area-A**				
1	neptune	**R**	**O**	**Y**	**G**
2	rootkit	**R**	**O**	**Y**	**G**
3	imap	**R**	**O**	**Y**	**G**
4	satan	**R**	**O**	**Y**	**G**
5	smurf	**R**	**O**	**Y**	**G**
6	normal	**R**	**O**	**Y**	**G**
7	pod	**R**	**O**	**Y**	**G**
8	neptune	**R**	**O**	**Y**	**G**
9	perl	**R**	**O**	**Y**	**G**
10	normal	**R**	**O**	**Y**	**G**
11	spy	**R**	**O**	**Y**	**G**
12	buffer_overflow	**R**	**O**	**Y**	**G**
13	smurf	**R**	**O**	**Y**	**G**
14	guess_passwd	**R**	**O**	**Y**	**G**
15	smurf	**R**	**O**	**Y**	**G**
16	smurf	**R**	**O**	**Y**	**G**
17	guess_passwd	**R**	**O**	**Y**	**G**
18	loadmodule	**R**	**O**	**Y**	**G**
19	portsweep	**R**	**O**	**Y**	**G**
20	land	**R**	**O**	**Y**	**G**
21	teardrop	**R**	**O**	**Y**	**G**
22	nmap	**R**	**O**	**Y**	**G**
23	loadmodule	**R**	**O**	**Y**	**G**
24	imap	**R**	**O**	**Y**	**G**
25	land	**R**	**O**	**Y**	**G**
26	spy	**R**	**O**	**Y**	**G**
27	rootkit	**R**	**O**	**Y**	**G**
28	loadmodule	**R**	**O**	**Y**	**G**
29	normal	**R**	**O**	**Y**	**G**
30	satan	**R**	**O**	**Y**	**G**

Part II - Scenario-I [A]
Scratch Paper

Work Role: _____ Respondent ID: _____

(Intentionally Left Blank)

Part III – Scenario-II [1b]

Scenario Threat Brief

Specific Situation: You are the IA security professional for Area-A's network security boundary. Various network security breaches are occurring in and around your locally defined area and throughout the wider-area's operational environment. . Each PPL recommendation chosen is an independent response.

Your Role: You decide the overall protective posture level (PPL) that should be assumed by Area-A in order to protect and defend your mission-critical resources IAW local policy. You use threat reports and context clues to support your decision when recommending the best PPL for your local Area.

Your goal: Recommend a PPL that you believe well allocates your protection resources' ability to mitigate the occurring threat and minimizes the cost of adverse effects on normal operations.

Local policy: Priority threats have the highest consideration for PPL recommendations. You should choose the PPL (i.e. red, orange, yellow or green) that you feel is best to mitigate the reported threat for the near-term future. PPL recommendations should be executed immediately.

Global Policy: Neighbor collaboration **IS** authorized.
You are aware that you have neighbors (Area-B, Area-C and Area-D, Area-F, Area-X) that may provide threat reports.

The following neighbor's threat reports about their protected resources are trustworthy:
(Area-B, Area-C, and Area-D).

Specific network vulnerabilities: These threats have a risk factor greater than or equal to 80% and have priority for threat mitigation within your security boundary;

Perl, rootkits, buffer_overflows, and **loadmodules**
signatures.
(See Figure 1 and 2)

SUMMARY:

Monitor the status of your active threat '***watch-list***'

Detect the status of occurring threats as reported.

Respond appropriately to operational environment threats by recommending the best protective posture to meet local goals and objectives. Indicate your response by circling RED, ORANGE, YELLOW or GREEN.

References, Figures 1, 2, 5 and 6.

Part III – Scenario-II [1b]
Example Questions and Discussion

Example Question 1.

	Credible IDPS Reports-i				Recommended Protective Posture			
Round	**Area-A**	**Area-B**	**Area-C**	**Area-D**				
23	*spy*	*perl*	*spy*	*satan*	**R**	**O**	**Y**	**G**

Discussion: Area A's IDPS is currently reporting/logging the detection of a *spy* threat. You consider all credible sources to include authorized neighbor reports, your own KSAs and policy guidance to make the best protective posture recommendation to mitigate the threat in the future.

	Credible IDPS Reports-i				Recommended Protective Posture			
Round	**Area-A**	**Area-B**	**Area-C**	**Area-D**				
23	*spy*	*perl*	*spy*	*satan*	**R**	**O**	**Y**	**G**

Clearly CIRCLE one PPL recommendation as R, O, Y or G.

Example Question 2.

	Credible IDPS Reports-i				Recommended Protective Posture			
Round	**Area-A**	**Area-B**	**Area-C**	**Area-D**				
7	*rootkit*	*rootkit*	*back*	*nmap*	**R**	**O**	**Y**	**G**

Discussion: Area A's IDPS is currently reporting/logging the detection of a *rootkit* threat. You consider all credible sources to include authorized neighbor reports, your own KSAs and policy guidance to make the best protective posture recommendation to mitigate the threat in the future.

	Credible IDPS Reports-i				Recommended Protective Posture			
Round	**Area-A**	**Area-B**	**Area-C**	**Area-D**				
7	*rootkit*	*rootkit*	*back*	*nmap*	**R**	**O**	**Y**	**G**

Clearly CIRCLE one PPL recommendation as R, O, Y or G.

Part III – Scenario-II [B]

Start: _____ END: _____

Work Role: _____ Respondent ID: _____

Instructions: Recommend the appropriate protective posture level (PPL) for each round in the table below by circling the best mitigation strategy for that threat. You should only select one choice per question. You are free to use scratch paper while taking this survey, but they must be turned in to the investigator at the end of the survey. Please clearly circle one and only one letter per response row.

R = RED, O = ORANGE, Y = YELLOW and G = GREEN See reference Figures 1, 2 and 3 if necessary

	Credible IDPS Reports-a				**Recommended Protective Posture**			
Round	**Area-A**	**Area-B**	**Area-C**	**Area-D**				
1	neptune	normal	multihop	multihop	**R**	**O**	**Y**	**G**
2	rootkit	land	phf	loadmodule	**R**	**O**	**Y**	**G**
3	imap	normal	back	phf	**R**	**O**	**Y**	**G**
4	satan	buffer_overflow	perl	loadmodule	**R**	**O**	**Y**	**G**
5	smurf	portsweep	pod	normal	**R**	**O**	**Y**	**G**
6	normal	satan	ipsweep	normal	**R**	**O**	**Y**	**G**
7	pod	ipsweep	loadmodule	buffer_overflow	**R**	**O**	**Y**	**G**
8	neptune	rootkit	multihop	ipsweep	**R**	**O**	**Y**	**G**
9	perl	portsweep	ipsweep	guess_passwd	**R**	**O**	**Y**	**G**
10	normal	phf	buffer_overflow	spy	**R**	**O**	**Y**	**G**
11	spy	rootkit	land	warezclient	**R**	**O**	**Y**	**G**
12	buffer_overflow	land	land	portsweep	**R**	**O**	**Y**	**G**
13	smurf	buffer_overflow	ipsweep	perl	**R**	**O**	**Y**	**G**
14	guess_passwd	warezclient	normal	spy	**R**	**O**	**Y**	**G**
15	smurf	ftp_write	portsweep	phf	**R**	**O**	**Y**	**G**
16	smurf	satan	neptune	ftp_write	**R**	**O**	**Y**	**G**
17	guess_passwd	perl	loadmodule	loadmodule	**R**	**O**	**Y**	**G**
18	loadmodule	satan	buffer_overflow	phf	**R**	**O**	**Y**	**G**
19	portsweep	ipsweep	rootkit	nmap	**R**	**O**	**Y**	**G**
20	land	neptune	imap	ftp_write	**R**	**O**	**Y**	**G**
21	teardrop	teardrop	guess_passwd	buffer_overflow	**R**	**O**	**Y**	**G**
22	nmap	neptune	ipsweep	pod	**R**	**O**	**Y**	**G**
23	loadmodule	multihop	buffer_overflow	warezmaster	**R**	**O**	**Y**	**G**
24	imap	rootkit	warezmaster	portsweep	**R**	**O**	**Y**	**G**
25	land	rootkit	multihop	loadmodule	**R**	**O**	**Y**	**G**
26	spy	neptune	satan	pod	**R**	**O**	**Y**	**G**
27	rootkit	spy	normal	loadmodule	**R**	**O**	**Y**	**G**
28	loadmodule	satan	perl	warezmaster	**R**	**O**	**Y**	**G**
29	normal	land	rootkit	multihop	**R**	**O**	**Y**	**G**
30	satan	smurf	multihop	nmap	**R**	**O**	**Y**	**G**

Part III – Scenario-II [B]

Scratch paper

Work Role: _____ Respondent ID: _____

Part IV - Respondent Reflection questions Overview

Instructions:

You are about to take Part-IV "Reflection Questions"

The purpose of the reflection questions is to allow you to provide insight into how you felt when making your protective posture decisions for scenarios I and II questionnaires.

You will be presented with nine multiple choice questions. You should carefully read each question and all of the available choices. After you have read the question and choices, briefly recall the scenarios that you just completed. Choose the best answer that most closely matches your response.

You may use scratch paper to add additional information if you would like.

Part IV – Respondent Reflection Questions

1. How **Confident** are you when making PPL recommendations given policy guidance?

- o 5 Extremely Confident
- o 4 Moderately Confident
- o 3 Somewhat Confident
- o 2 A little Confident
- o 1 Not at all Confident

2. How well did a lack of knowledge of credible **neighbor resources** help in determining your PPL recommendations?

- o 5 Definitely Helped
- o 4 Somewhat Helpful
- o 3 No effect
- o 2 Not very helpful
- o 1 Definitely unhelpful

3. How well did credible neighbors help the **situational awareness** of your local environment?

- o 5 Definitely Helped
- o 4 Somewhat Helpful
- o 3 No effect
- o 2 Not very helpful
- o 1 Definitely unhelpful

4. How well did credible neighbor reports help your **confidence level** in **question 1?**

- o 5 Extremely helpful
- o 4 Moderately helpful
- o 3 Somewhat helpful
- o 2 A little helpful
- o 1 Not at all helpful

5. How helpful was knowledge **of credible neighbor resources** in making PPL recommendations?

- o 5 Definitely Helped
- o 4 Somewhat Helpful
- o 3 No effect
- o 2 Not very helpful
- o 1 Definitely unhelpful

6. How well did credible neighbors help the **situational awareness** of your global environment?

- o 5 Definitely Helped
- o 4 Somewhat Helpful
- o 3 No effect
- o 2 Not very helpful
- o 1 Definitely unhelpful

7. How helpful were **neighbor threat reports** when considering PPL recommendations?

- o 5 Definitely Helped
- o 4 Somewhat Helpful
- o 3 No effect
- o 2 Not very helpful
- o 1 Definitely unhelpful

8. How helpful is **multiple neighbor reports of the same threat** when making PPL recommendations?

- o 5 Definitely Helped
- o 4 Somewhat Helpful
- o 3 No effect
- o 2 Not very helpful
- o 1 Definitely unhelpful

9. When recommending PPLs, how would you rate the **value of having credible neighbors to collaborate with?**

- o 5 Extremely Valuable
- o 4 Moderately Valuable
- o 3 Somewhat Advantageous
- o 2 A little Valuable
- o 1 Not at all Valuable

Protective Posture Level (PPL) Response Action	Operating Cost	PPL Response Action Description
RED (Immi-nent) deliberate	Extremely High	The local IDPS's reported status of an active threat or a preconfigured sequence indicates an imminent threat that could cause significant loss to *mission-critical* resources. This PPL requires **deliberate** threat mitigation and avoidance actions. To, reduce potential losses, IAW policy, you should: o Immediately deploy QRF resources to contain and mitigate this threat. o Significantly restrict all in-bound traffic flow o Conduct deep packet inspections of in-bound *mission-critical* traffic o Update active '*watch-list*' o Remain vigilant for near-term/future/persistent threats o Monitor, detect and report status to meet organizational goals
ORANGE (Significant) specific	High	IDPS(s)'s reported status of an active threat or a preconfigured sequence indicates a significant threat to *mission-critical* resources. The threat is not detected by local IDPS; however, additional credible information indicates a correlation that you may still be locally vulnerable to this active threat in the near-term. This PPL requires **specific** threat mitigation and avoidance actions. To, reduce potential losses, IAW policy, you should: o Place QRF resources on standby o Slow in-bound traffic flow for *mission-critical* resources o Random deep-packet inspections of inbound *mission-critical* traffic o Update active '*watch-list*' o Remain vigilant for near-term/future/persistent threats o Monitor, detect and report status to meet organizational goals
YELLOW (Moderate) random	Medium	IDPS(s)'s reported status of an active threat or a preconfigured sequence indicates a moderate threat to locally protected resources. This PPL requires **random** threat mitigation and avoidance actions. To, reduce potential losses, IAW policy, you should: o Random threat mitigation actions (i.e. QRF alert-recall, off-peak deep packet inspections, other access control audits.) o Modify pace of specified in-bound traffic flows o Update '*watch-list*' o Remain vigilant for near-term/future/persistent threats o Monitor, detect and report status to meet organizational goals
GREEN (Minimal) normal	Low	IDPS(s)'s reported posterior probability of an actionable threat was not sufficient for the employment of additional threat mitigation resources during this period. This PPL requires **normal** threat mitigation and avoidance actions. To, reduce potential losses, IAW policy, you should: o Update '*watch-list*' o Maintain normal operations for the next period. o Monitor, detect and report status to meet organizational goals No additional resources are deployed.

Figure 24. Intrusion detection alert and response matrix

KDD99 Threat Label	Category Description/Definition
buffer_overflow	Unauthorized access to a local *superuser* or (root) privileges.
loadmodule	
perl	
rootkit	
ftp_write	Unauthorized access from a remote machine.
guess_passwd	
imap	
multihop	
phf	
spy	
warezclient	
warezmaster	
back	Denial of Service
land	
neptune	
pod	
smurf	
teardrop	
ipsweep	Probing: Surveillance and other probing.
nmap	
portsweep	
satan	
normal	Normal Traffic

Figure 25. KDD99-specific categorized threat label definition.

Protected Resource Assets	
	Area-A
Core router	MC
IDS	MC
Web Server	X
Secure Data Storage	MC
SCADA power system	MC
Software Storage	MC
Desktop	X
Call Manager Cluster (non-secure)	X
Call Manager Cluster (Secure)	MC
Video Server	X

Figure 26. Resource List for Area-A

In Figure 3, an, 'X' indicates that the network actively monitors, detects and reports the threat status for this resource. A 'MC' indicates that the organization has determined this protected resource as a high priority mission-critical resource. A marking of 'na' indicates that the network does not provide protection for that resource type. For example, Area-A is providing intrusion detection services for all of the resource types except for 'Mobile Device'. In addition, the Core router, IDS, Secure Data Storage, and Secure Call-manager Cluster have been determined to be mission-critical high-priority assets for threat mitigation and avoidance response actions.

Protected Resource Assets	Network Security Boundary			
	Area-A	Area-B	Area-C	Area-D
Core router	MC	MC	MC	MC
IDS	MC	MC	MC	MC
Web Server	X	MC	X	X
Secure Data Storage	MC	MC	MC	X
SCADA power system	MC	X	X	MC
Software Storage	MC	X	X	MC
Desktop	X	MC	X	MC
Call Manager Cluster (non-secure)	X	MC	MC	X
Call Manager Cluster (Secure)	MC	X	MC	MC
Video Server	X	MC	MC	X

Figure 27. Credible Neighbor Resource List for Area-A

In Figure 3, an, 'X' indicates that the network actively monitors, detects and reports the threat status for this resource. A 'MC' indicates that the organization has determined this protected resource as a high priority mission-critical resource. A marking of 'na' indicates that the network does not provide protection for that resource type. For example, Area-A is providing intrusion detection services for all of the resource types except for 'Mobile Device'. In addition, the Core router, IDS, Secure Data Storage, and Secure Call-manager Cluster have been determined to be mission-critical high-priority assets for threat mitigation and avoidance response actions.

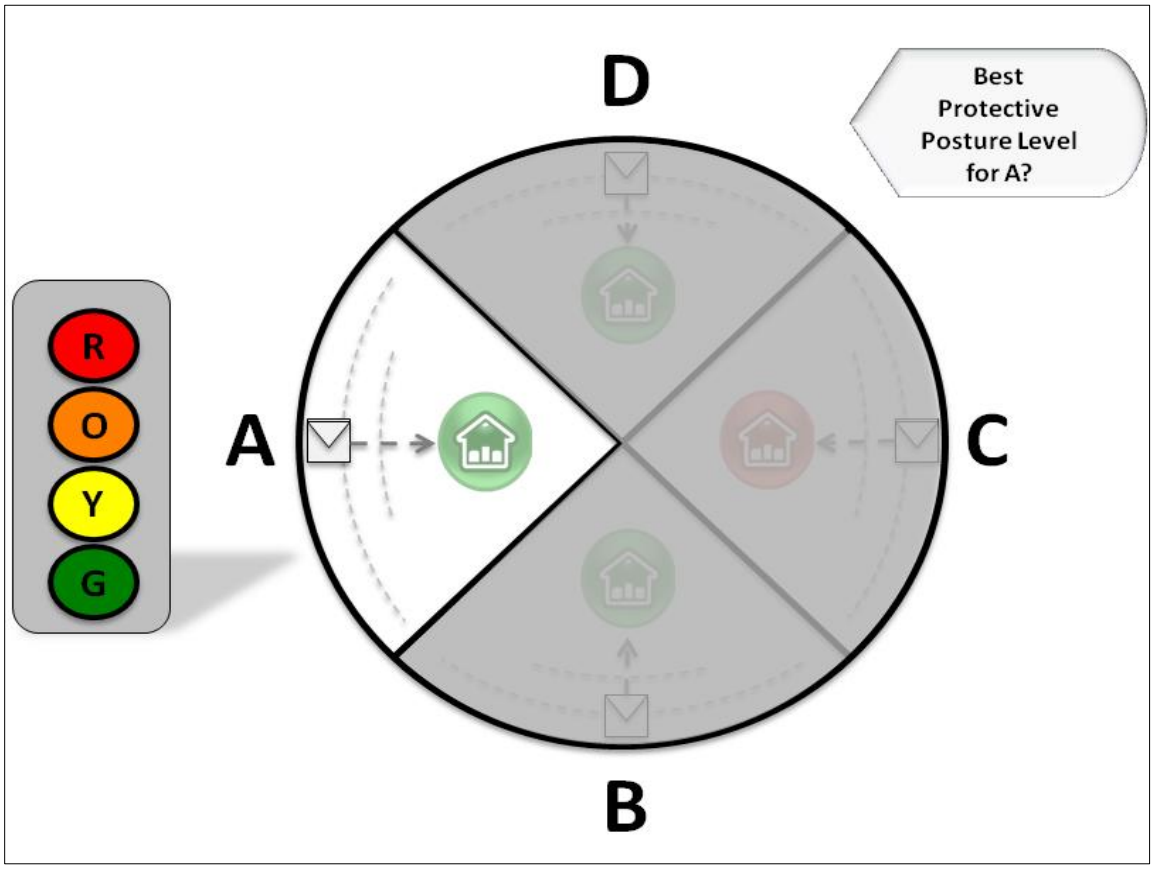

Figure 28. Isolated Threat Awareness Mitigation Model.

The outer-edge of the circle symbolizes the global operational environment for network security boundary protection and it is divided into four local areas, (Areas A, B, C and D). The un-trusted area for local decisions is shaded in gray (Areas B, C and D). Area-A represents the current trusted local perspective and awareness of the global threat. In this model, Area-A may be aware of other security analysts in the operational environment however; their trustworthiness has not been determined, they are not authorized to collaborate with off-site or non-credible entities; or sources are authorized, but real-time communications is not secure or unavailable for timely decision-support.

As the packets enter the network security boundary the IDPS reports the status and threat label to the operator. The operator evaluates the report and makes a recommendation to best mitigate the threat for the current and near-term future.

The IA security professional should not consider information from shaded areas while recommending the best threat mitigation protective postures for their local network security boundary.

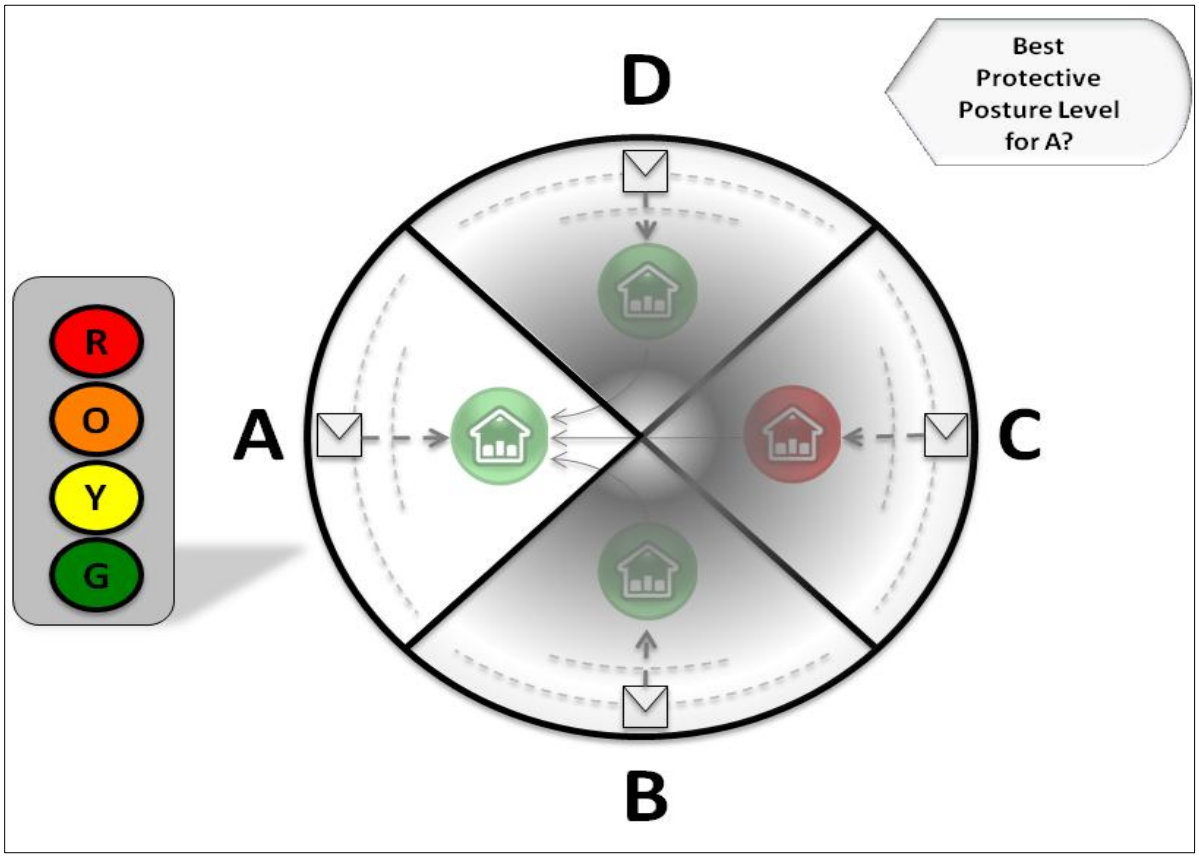

Figure 29. Collaborative Threat Awareness Mitigation Model:

The outer-edge of the circle symbolizes the global operational environment for network security boundary and it is divided into four local areas, (Areas A, B, C and D). This model is focused more on the credibility of the reported threat event itself, not the credibility of the reporter/operator or how the local area responded to the event. The threat events that are being reported have been determined to be credible and trustworthy by participating neighbors. Area-A represents the current local perspective of interest for threat mitigation and prevention. You can assume that a real-time network provides timely collaboration and threat information sharing across a secure communications network.

As packets enter the network security boundary the IDPS reports the status and threat label are presented to Area-A's local operator and the artificial neural network (ANN) which symbolizes the global threat reporter. The operators evaluate their local threat report and consider the global threat reports from their neighboring sources to best mitigate the threat for the current and near-term future.

The IA security professional should consider information from shaded areas while recommending the best threat mitigation protective postures for their local network security boundary.

Date: 20 JULY 2014

MEMORANDUM FOR

FROM: AFIT/ENG
2950 Hobson Way
Wright Patterson AFB OH 45433-7765

SUBJECT: Request for Staff, Student and Faculty participation in decision-support survey study and graduate research support

Dear [student name]:

I am writing to request your help with an important human subjects study. MAJ Tyrone Lewis is conducting a study to support his thesis entitled; *Modeling Integrated Network Security Boundaries as Complex Adaptive Systems*. MAJ Lewis is a Cyber Operations Student that is expected to graduate in August.

Survey Purpose: Gather elements that you, as the respondent, consider most critical when making decisions in an intrusion detection and prevention networking scenario. The survey is UNCLASSIFIED, anonymous and no personal identifiable information will be recorded or kept on file.

Target Audience: Personnel with Information Assurance experience and related network defense roles are preferred, however not required.

Estimated time: Approximately 30 minutes
Survey Format: This is a four part anonymous study to determine the effects of event collaboration on human decision-support profiles. In Part-I, respondents are asked to complete baseline information and introduced to the materials that will be used during the survey. Participants are faced with a network threat scenario during Part-II, and are expected to recommend a protective posture that best protects their local-area network security boundary. The conditions are slightly modified and respondents are surveyed again during Scenario-III. Finally, in Part IV (Participant Reflection) questions are asked to determine if there was a change in their recommendation considerations. Following the closing of the survey, respondents are asked to participate in an after action review and provide feedback.

Location: TBD

SUBJECT: Request for Staff, Student and Faculty participation in decision-support survey study and graduate research support

The survey will be conducted in a classroom environment using pencil and paper as the instruments for recording responses. The exact room number will be provided after you have registered for a time-slot.

When: The survey will be conducted from: July 24, 2014 until August 8, 2014.

Preliminary Results will be presented on 20AUG14 during the student Thesis Defense.

If you are interested we welcome you to participate in this survey by reserving your 30 minute time-slot today.

Informed consent: All subjects are self-selected to volunteer to participate in this survey interview. No adverse action is taken against those who choose not to participate. Subjects are made aware of the nature and purpose of the research, sponsors of the research, and disposition of the survey results. A copy of the Privacy Act Statement of 1974 is presented for their review.

4. If you have any questions about this request, please contact Maj Brian G. Woolley, PhD (primary investigator) – Phone 255-3636, ext. 4618; E-mail: brian.woolley@afit.edu.

Maj Brian G. Woolley, PhD
Principal Investigator

Date: 9 JULY 2014

MEMORANDUM FOR AFIT IRB Reviewer

FROM: AFIT/ENG
2950 Hobson Way
Wright Patterson AFB OH 45433-7765

SUBJECT: Request for exemption from human experimentation requirements (32 CFR 219, DoD 3216.2 and AFI 40-402) for Protective Posture Recommendation Profiles

1. The purpose of this survey is to gather situation awareness requirements data that IA security professionals need when making threat mitigation decisions. The requirements data may include the operator's preferences for threat identification methods, the status of the threat relative to time and space, the meaning of the threat's status in the context of the operational environment and the operator's best recommendation for threat mitigation responses IAW local policy tactics techniques and procedures.

a) Intent: The results will support the student's graduate level research.

b) Objectives: Determine if the recommendation profiles from the respondents can be encoded into the Artificial Neural Network (ANN) in a manner that enhances situation awareness. The results of the requirements encoding will be used to determine the ANN's performance and how well it can accurately represent the generalized profiles. The performance results of the ANN will be included in further research recommendations that include recommendations for threat mitigation and collaboration suggestions for enhanced situation awareness.

2. This request is based on the Code of Federal Regulations, title 32, part 219, section 101, paragraph (b) (2) Research activities that involve the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures, or observation of public behavior unless: (i) Information obtained is recorded in such a manner that human subjects can be identified, directly or through identifiers linked to the subjects; and (ii) Any disclosure of the human subjects' responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation.

3. The following information is provided to show cause for such an exemption:

a) Equipment and facilities: A standard classroom, chairs, tables, pen and paper are needed to support this survey.

b) Source of subjects: AFIT Faculty, Staff, and Students

Total Number: 20

Inclusion/exclusion: IA Security Professionals of various backgrounds. Do not include personnel that have never heard of Information Assurance.

Age range: No restrictions.

c) Timeframe: Two weeks

d) Data collected: This study will not collect personal identifiers or specific demographic information. The data will be collected by a combination of interview and survey that will be administered by the assistant investigator. See enclosures 1 and 2.

e) Risks to Subjects: Subjects may disclose tactics techniques and procedures that are of a classified nature. Subjects will be notified that the entire survey is UNCLASSIFIED. If a subject's future response reasonably places them at risk of criminal or civil liability or is damaging to their financial standing, employability, or reputation, I understand that I am required to immediately file an adverse event report with the IRB office. I understand that the names and associated data I collect must be protected at all times, only be known to the researchers, and managed according to the AFIT interview protocol. All interview data will only be handled by the following researchers (MAJ Tyrone Lewis and MAJ Woolley). At the conclusion of the study, all data will be turned over to the advisor and all other copies will be destroyed.

f) Informed consent: All subjects are self-selected to volunteer to participate in the interview. No adverse action is taken against those who choose not to participate. Subjects are made aware of the nature and purpose of the research, sponsors of the research, and disposition of the survey results. A copy of the Privacy Act Statement of 1974 is presented for their review.

4. If you have any questions about this request, please contact Maj Brian G. Woolley, PhD (primary investigator) – Phone 255-3636, ext. 4618; E-mail: brian.woolley@afit.edu.

Maj Brian G. Woolley, PhD
Principal Investigator

Attachments:
1. Survey questions
2. Interviewer questions

Bibliography

Anderson, J. O. (1980). *Computer Threat Monitoring and Surveillance.* Fort Washington: James P. Anderson Consulting Co.

Army. (2004). *Training Analysis: Systems Approach to Training Analysis* (Vols. Tradoc Pamphlet 350-70-6). Fort Monroe, VA: HQ, Department of the Army, U.S.

Army, U. D. (2005). *Military Decision making Process, Army Planning and Orders Production. Field Manual 5-0 (FM 101-5).* Washington, DC:: U.S. Department of the Army.

Bace, R. G. (2000). *Intrusion Detection.* Indianapolis: Macmillan Technical Publishing.

Bar-Yam, Y. (1997). *Studies in Nonlinearity; Dynamics of Complex Systems.* (R. L. Devaney, Ed.) Boulder, CO: Westview Press.

BUI, T. X. (1986). *Communications Desgin for Co-Op" A Desion Support System.* New Your, University: Naval Postgraduate School.

Carter, E. (2006). *CCSP Intrusion Prevention Systems, Self-Study.* (J. kane, Ed.) Indianapolis, Indiana, United States of America: Cisco Press.

Cisco. (2012, September). *Cisco IPS 4500 Series Sensors Performance of Cisco IPS 4500 and 4300 Series Sensors.* Retrieved April 15, 2014, from www.cisco.com: http://www.cisco.com/c/en/us/products/collateral/security/ips-4500-series-sensors/white_paper_c11-716084.pdf

Defense, D. o. (2001). *DoD Antiterrorism Standards.* Instruction, Defense.

Denning, D. E. (1986). An Intrusion-Detection Model. *IEEE Transactions on Software Engineering*.

Department of the Army, U. (2014). *Cyber Electromagnetic Activities* (Vols. FM 3-38). Washington, DC: U.S. Department of the Army.

Easley, D., & Kleinberg, J. (2010). *Networks Crowds and Markets: Reasoning about a Highly Connected World.* New York, New York, United States of America: Cambridge.

Endsley, M. R., & Bolte, B. J. (2003). *Designing for Situation Awareness; An Approach to User-Centered Design.* New Your, NY: Taylor & Francis.

Endsley, M. R., & Garland, D. J. (2000). *Situation Awareness Analysis And Measurement.* Boca Raton: Lawrence Erlbaum Associates, Inc.

Floreano, D., & Mattiusi, C. (2008). *Bio-Inspired Artificial Intelligence: Theories, Methods, and Technologies.* (R. C. Arkin, Ed.) Cambridge, Massachusetts, United States of America: MIT Press.

Hart, J. L. (2005, March). *An Historical Analysis of Factors Contributing to the Emergence of the Intrusion Detection Discipline and its Role in Information Assurance.* MS thesis, Graduate Scool of Management and Engineering, Air Force Institute of Technology (AU), AFIT/GIR/ENV/05M-06, Wright-Patterson AFB OH.

Headquarters, D. o. (2012). *The Operations Process: Army Doctrine Publication 5-0 (FM 5-0).* Washington, DC: U.S. Department of the Army.

Heaton, J. (2012, may 17). Introduction to the Math of neural Networks. Heaton Research Inc.

Hettich, S., & Bay, S. (1999). *kdd.ics.uci.edu.* Repository, University of California, Department of Information and Computer Science, Irvine.

Hodgkin, A., & Huxley, A. (1952). A Quantative Description of Membrane Current and its Application to Conduction and Excitation in Nerve. *Jouranl of Physiology*(108), 500-544.

Holland, J. H., & Miller, J. H. (1991, May). Artificial Adaptive Agents in Economic Theory. *American Economic Association, 81*(2), 365-370.

Jontz, S. (2014, August). The Future of Modeling and Simulation for U.S. Army Tactical Networks. (R. K. Ackerman, Ed.) *Signal, 68*(12), 25-27.

Lewes, G. H. (1875). *Problems of Life and Mind: Third Series. .* Hong Kong: Forgotten Books. (Original work published 1879).

Lewis, T. G. (2009). *Network Science: Theory and Applications.* Hoboken, New Jersey, United States of America: Wiley.

Lyons, K. B. (2014, March). *A Recommender System in the Cyber Defense Domain.* MS-Thesis, Graduate Scool of Management and Engineering, Air Force Institute of Technology (AU), AFIT-ENG-14-M-49, Wright-Patterson AFB.

McCulloch, W., & Pitts, W. (1943). A Logical Calculus of the Ideas Immanent in Nervous Activity. *Bulletin of Mathematical Biophysics*(5), 115-133.

Miller, J. H., & Page, S. E. (2007). *Complex Adaptive Systems.* Princeton, New Jersey, United States of America: Princeton University Press.

Mitchell, T. M. (1997). Machine Learning. (C. Liu, Ed.) 81-123, 110-112,111.

NIST. (2014 йил 18-August). *National Institute of Standards and Technology*. From National Vulnerabilities Database: http://nvd.nist.gov/cvss.cfm

Opit, D. (1999, August). Popular Ensemble Methods: An Empirical Study. *Journal of Artificial Intelligence Research*.

Phister, P. W. (2010, April 9). Cyberspace: The Ultimate Complex Adaptive System. (D. S. Alberts, Ed.) *The International C2 Journal, IV*(2).

Pipken, D. L. (2000). *Information Security: Protecting the Global Enterprise.* Upper Saddle River, NJ, USA: Prentice Hall.

Quammen, D. (2008). *Charles Darwin: On the Origin of Species The Illustrated Edition.* New York, NY: Sterling.

Raulerson, E. L. (2013, March). *Modeling cyber Situational Awareness Through Data Fusion.* MS-Thesis, Graduate of School of Management and Engineering, Air Force Institute of Technology (AU), AFIT/ENG/13/M/41, Wright-Patterson Air Force Base.

Renze, J., & Weisstein, E. W. (2014). *Law of Large numbers.* Retrieved 08 13, 2014, from Mathworld: http://mathworld.wolfram.com/LawofLargeNumbers.html

Scarfone, K. A., & Mell, P. M. (2007, February 20). *Guide to Intrusion Detection and Prevention Systems (IDPS): Special Publication 800-94.* Retrieved July 10, 2013, from National Institute of Standards and Technology: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=50951

Skinner, B. (2005). *Science and Human Behavior.* Pearson Education, INC.

Svenson, P., & Sidenbladh, H. (n.d.). Determining Possible Avenues of Approach Using ANTS. *6th international Conference on Information Fusion* (pp. 1110-1117). Stockholm, Sweden: Swedish Defence Research Agency.

Symantec. (2014). Internet security Threat Report 2014. *ISTR, 19.*

Turof, M. (1975). *The Delphi Method: Techniques and Applications.* (H. A. Linstone, Ed.) Addison-Wesley Publishing Co.

U.S. Army, D. o. (2011). *Department of Defense Strategy for Cyberspace.* Washington, DC, U.S.: U.S. Department of the Army.

Wade Norman, M. (2010). *The Battle Staff: The Essentials of Warfighting Smartbooks* (Vol. 3). Lakeland, FL: Lightning Press.

Ware, W. H. (1970). *Security Controls for Computer Systems (U): Report of Defense Science Board Task Force on Computer Security.* The RAND Corporation, Office of the Director of Defense Research and Engineering. Washington: The RAND Corporation.

Wilensky, U. (2006). Perceptron Model. *NetLogo. http://ccl.northwestern.edu/netlogo/. Center for Connected Learning and Computer-Based Modeling.* Evanston, IL.

Wilensky, U. (2013, March 19). *NetLogo User Manual.* Retrieved May 12, 2013, from Netlogo: http://ccl.northwestern.edu/netlogo/docs/

Williams, R. J. (1986). The Logic of Activation Functions. In D. Rumelhart, & J. McClelland, *Parallel Distributed Processing, Explorations in the Microstructure of Cognition, Vol. 1 Foundations* (Vol. 10). Cambridge, MA: PDP Research Group.

Williams, R., Rumelhart, D., & McClelland, J. (1986). *The Logic of Activation Functions, chapter 10 in Parallel Distributed Processing, Explorations in the Microstructure of Cognition* (Vol. 1). Cambridge, MA: PDP Research Group.

Vita

Major Tyrone A. L. Lewis graduated from Central high school in Springfield Missouri. He joined the Army in 1996 as a Private and was quickly promoted through the ranks to Staff Sergeant in 2001. After being selected for Officer Candidate School, he was commissioned at Fort Benning Georgia in 2002 and recognized as a Distinguished Honor Graduate. He graduated Magna Cum Laude from the University Of Maryland University College in College Park, Maryland with a Bachelor of Science degree in Management Studies in 2004.

In his first assignment he led a platoon of 135 Soldiers in the direct support maintenance of M1A1 and M1A2 tanks for 3 Corps Field Artillery, and was recognized for integrating logistical systems which corrected a two year inventory deficiency and reduced the maintenance back log by over 30% as the Maintenance Control Officer. He graduated from the Army's Telecommunications Systems Engineer Course in 2006, and deployed to Iraq as the junior network engineer for 3rd Infantry Division during the *surge*. His highest award, The Bronze Star, was received for his engineering contributions to include a fiber-based communications infrastructure design for enduring forward operating base Delta. He received the Rowan Award for his design and demonstration of Fort Gordon Georgia's Installation-wide Signal Training Network in 2010. He was promoted below the zone to Major in 2011. In August 2012, he began graduate studies in Cyber Operations at the Air Force Institute of Technology (AFIT). Upon graduation, he will continue his studies at AFIT in pursuit of a Doctoral degree in Computer Science.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From – To)*
18-08-2014	Master's Thesis	August 2012 – September 2014

TITLE AND SUBTITLE

An Artificial Neural Network-based Decision-Support System for Integrated Network Security

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lewis, Tyrone A. L. Sr., Major, USA

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)
Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-8865

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/ENG/T-14-S-09

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Intentionally left blank

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
DISTRUBTION STATEMENT A. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

As large-scale Cyber attacks become more sophisticated, local network defenders should employ strength-in-numbers to achieve mission success. Group collaboration reduces individual efforts to analyze and assess network traffic. Network defenders must evolve from an isolated defense in sector policy and move toward a collaborative strength-in-numbers defense policy that rethinks traditional network boundaries. Such a policy incorporates a network watch approach to global threat defense, where local defenders share the occurrence of local threats in real-time across network security boundaries, increases Cyber Situation Awareness (CSA) and provides localized decision-support. A single layer feed forward artificial neural network (ANN) is employed as a global threat event recommender system (GTERS) that learns expert-based threat mitigation decisions. The system combines the occurrence of local threat events into a unified global event situation, forming a global policy that allows the flexibility of various local policy interpretations of the global event. Such flexibility enables a Linux based network defender to ignore windows-specific threats while focusing on Linux threats in real-time. In this thesis, the GTERS is shown to effectively encode an arbitrary policy with 99.7% accuracy based on five threat-severity levels and achieves a generalization accuracy of 96.35% using four distinct participants and 9-fold cross-validation.

15. SUBJECT TERMS
Cyberspace security professional, Artificial neural networks, intrusion detection, collaboration, network defender, global threat event recommender system, decision-support, security boundaries

16. SECURITY CLASSIFICATION OF: U			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Brian G. Woolley, MAJ, PhD, Advisor, AFIT/ENG
U	**U**	**U**	**UU**	170	**19b. TELEPHONE NUMBER** *(Include area code)* (937) 255-6565, ext 4618 (NOT DSN) (brian.woolley@afit.edu)

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18