Calhoun

Institutional Archive of the Naval Postgraduate School

Calhoun: The NPS Institutional Archive

Theses and Dissertations	Thesis Collection

2013-03

A DEFINITIVE INTEROPERABILITY TEST METHODOLOGY FOR THE MALICIOUS ACTIVITY SIMULATION TOOL (MAST)

Hayes, Nathaniel J.

Monterey, California. Naval Postgraduate School

NAVAL
POSTGRADUATE
SCHOOL

MONTEREY, CALIFORNIA

THESIS

**A DEFINITIVE INTEROPERABILITY TEST
METHODOLOGY FOR THE MALICIOUS ACTIVITY
SIMULATION TOOL (MAST)**

by

Nathaniel J. Hayes

March 2013

Thesis Advisor: Gurminder Singh
Co-Advisor: John H. Gibson

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE March 2013	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE A DEFINITIVE INTEROPERABILITY TEST METHODOLOGY FOR THE MALICIOUS ACTIVITY SIMULATION TOOL (MAST)		5. FUNDING NUMBERS	
6. AUTHOR(S) Nathaniel J. Hayes			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		10. SPONSORING/MONITORING AGENCY REPORT NUMBER	

11. SUPPLEMENTARY NOTES   The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.   IRB Protocol number ___N/A_____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE A

13. ABSTRACT (maximum 200 words)

The threat of degradation or disruption from cyber infiltration, espionage, and theft to militarily and nationally critical information and network systems poses a significant challenge to DoD and DON. To mitigate this challenge, network administrators must be trained to properly recognize and defend against malicious activity.

The Malicious Activity Simulation Tool (MAST), a software program under development at NPS, mimics the behavior and impact of network-based malware in an effort to train the administrators of operational DoD networks both to respond to the threats such materials present to their networks and to assess their competence in recognizing and responding to such threats.

In order for MAST to achieve its potential as an acceptable assessment and training tool, it must first be shown to present no new threat to the environment for which it was designed. This thesis develops a step-by-step testing procedure, the execution of which will demonstrate that MAST can perform at a level commensurate with current criteria for operating securely on DoD networks.

Additionally, this thesis discusses the quantitative testing environment and current testing and implementation methods and criteria for new cyber hardware and software programs of record in the DoD.

14. SUBJECT TERMS Malware, Quantitative Testing, Computer Network Defense, Simulation, Network Administrator Training, Cyberspace, Cyber Domain, Cyber Test Range	15. NUMBER OF PAGES 119
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU

THIS PAGE INTENTIONALLY LEFT BLANK

A DEFINITIVE INTEROPERABILITY TEST METHODOLOGY FOR THE MALICIOUS ACTIVITY SIMULATION TOOL (MAST)

Nathaniel J. Hayes
Lieutenant, United States Navy
B.A., University of Washington, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2013

Author: Nathaniel J. Hayes

Approved by: Gurminder Singh
               Thesis Advisor

               John H. Gibson
               Thesis Co-Advisor

               Cynthia E. Irvine
               Chair, Cyber Academic Group

iii

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The threat of degradation or disruption from cyber infiltration, espionage, and theft to militarily and nationally critical information and network systems poses a significant challenge to DoD and DON. To mitigate this challenge, network administrators must be trained to properly recognize and defend against malicious activity.

The Malicious Activity Simulation Tool (MAST), a software program under development at NPS, mimics the behavior and impact of network-based malware in an effort to train the administrators of operational DoD networks both to respond to the threats such materials present to their networks and to assess their competence in recognizing and responding to such threats.

In order for MAST to achieve its potential as an acceptable assessment and training tool, it must first be shown to present no new threat to the environment for which it was designed. This thesis develops a step-by-step testing procedure, the execution of which will demonstrate that MAST can perform at a level commensurate with current criteria for operating securely on DoD networks.

Additionally, this thesis discusses the quantitative testing environment and current testing and implementation methods and criteria for new cyber hardware and software programs of record in the DoD.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACAS	Assured Compliance Assessment Solution
ADNS	Automated Digital Network System
AFB	Air Force Base
BLII	Base Level Infrastructure Information
C4	Command, Control, Communications, and Computers
C4I	Command, Control, Communications, Computers and Intelligence
CANES	Consolidated Afloat Networks and Enterprise Services
CC/S/A	Combatant Commands, Services, and Agencies
CCE	Common Computing Environment
CDC	Community Data Center
CENTRIXS	Combined Enterprise Regional Information Exchange System
CIO	Chief Information Officer
CNCI	Comprehensive National Cybersecurity Initiative
CND	Computer Network Defense
CND-IAS	Computer Network Defense Information Assurance Suite
CND-OSE	Computer Network Defense Operating System Environment
CNTT	Computer Network Team Trainer
COMPOSE	Common PC Operating System Environment
COMPTUEX	Composite Training Unit Exercise
CoSC	Continuity of Services Contract
COTS	Commercial Off-the-Shelf
CPU	Central Processing Unit
DDG	Guided Missile Destroyer
DISA	Defense Information Systems Agency
DNI	Director of National Intelligence

DNS	Domain Name System
DoD	Department of Defense
DoDIAR	Department of Defense Information Assurance Range
DON	Department of the Navy
DON CIO	Department of the Navy Chief Information Officer
DoS	Denial of Service
EOL	End-of-Life
FY	Fiscal Year
GIG	Global Information Grid
GOTS	Government Off-the-Shelf
GUI	Graphic User Interface
HBSS	Host Based Security System
HIDS	Host Intrusion Detection System
HIPS	Host Intrusion Prevention System
HQMC	Headquarters Marine Corps
HSPD	Homeland Security Presidential Directive
HW	Hardware
IA	Information Assurance
IASM	Intelligent Agent Security Module
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Manager
IP	Internet Protocol
ISNS	Integrated Shipboard Network System
IT	Information Technology
IT-21	Information Technology for the 21st Century
JCOR/SIMTEX	Joint Cyber Operations Range/Simulator Training and Exercise
JIOR	Joint Information Operations Range
MAST	Malicious Activity Simulation Tool
MM	Malware Mimic
NCDOC	Navy Cyber Defense Operations Command

NCOR	Navy Cyberspace Operations Range
NCR	National Cyber Range
NEN	Naval Enterprise Networks
NGEN	Next Generation Enterprise Network
NIDS	Network Intrusion Detection System
NIOC	Navy Information Operations Command
NMCI	Navy Marine Corps Intranet
NOC	Navy Operations Center
NPS	Naval Postgraduate School
NSPD	National Security Presidential Directive
OCONUS	Outside of the Continental U.S.
OCRS	Online Compliance Reporting System
ONE-Net	OCONUS Navy Enterprise Network
OOL	Out-of-Limits
OS	Operating System
PDC	Primary Domain Controller
PEO	Program Executive Office
PEO C4I	Program Executive Office for Command, Control, Communications, Computers and Intelligence
PEO-EIS	Program Executive Office for Enterprise Information Systems
PEO-MA	Program Executive Office for Mission Assurance
PMW	Program Manager, Warfare
POC	Point of Contact
POR	Program of Record
PPL/SSIL	Preferred Product List/System Subsystem Interface List
SCCVI	Secure Configuration Compliance Validation Initiative
SCI	Sensitive Compartmented Information
Simware	Simulated malware
SIPR	Secure Internet Protocol Router

SIPRNet	Secure Internet Protocol Router Network
SOVT	System Operational Verification Test
SPAWAR	Space and Naval Warfare Systems Command
STIG	Security Technical Implementation Guide
STRATCOM	Strategic Command
SW	Software
TBD	To be Determined
TCP	Transmission Control Protocol
TS	Top Secret
TS/SCI	Top Secret/Sensitive Compartmented Information
TTP	Tactics, Techniques, and Procedures
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VRAM	Vulnerability Remediation Asset Manager
WAN	Wide Area Network

ACKNOWLEDGMENTS

I dedicate this thesis to my grandfather in whose magnificent shadow I will forever labor.

And to John, for not giving up.

I would like to acknowledge Dr. Gurminder Singh, my thesis advisor, for his professional guidance, expertise, and patience. Thank you also goes to my co-advisor Mr. John Gibson, for helping me to maintain focus and without whom I would certainly have fallen victim to my own poor grammar.

This work would not have been complete without the contributions of my department chair Dr. Cynthia Irvine, and the MAST group: Taff, Salevski, Neff, Arijit, Longoria, Littlejohn, Makhlouf, Belli, and Lowney. Thank you for letting me contribute to this great project.

There is a group of people who consistently drive me to succeed, and I owe them thanks for providing motivation during this long project. Thank you to my brothers and sisters, every one of you. A heartfelt "thank you" goes to my wife's mother, for her tireless diligence and kindness.

To my friends who have studied alongside me: Mate, Nick, Billy, and Jerry. Thanks for making this time enjoyable.

Finally, to my beautiful, intelligent, and loving wife, Yasmine: I love you. You are my lighthouse beaconing from solid rock that no amount of sea or weather can extinguish or stop from bringing me safely home.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Establishing trust in Department of Defense (DoD) network durability against attack, and actively maintaining that trust, is crucial to the success of networked operations. Such operations are the heart of DoD doctrine. It is a reality of 21st-centry warfare that a variety of cyber activities from varying sources can compromise security and adversely affect a command, platform, the Navy, or DoD as a whole.

The activities that leverage these system vulnerabilities can be intentional or unintentional. Intentional exploits are those that are targeted and untargeted attacks from any malicious actor, be it a state, criminal organization, or individual. An example of an unintentional vulnerability is one that is caused by failure to follow proper network security procedures, such as installing software upgrades or patches [1]. Targeted actions against networks are potentially devastating, because the targeted attack is more likely intended to exploit known vulnerabilities. It is especially disheartening if the exploit takes advantage of vulnerabilities for which there are existing solutions [2].

The potential impact of these vulnerabilities is amplified by the connectivity between systems, the Internet, and the Global Information Grid (GIG), providing the adversary an avenue of approach. The Navy and DoD continue to move to networked operations, increasing the exposure of cyber vulnerabilities to potential exploits and malicious activities.

In February 2011, the Director of National Intelligence (DNI) testified that in the previous year there had been a dramatic increase in malicious cyber activity targeting U.S. computers and networks, including a more than tripling of the volume of malicious software since 2009 [3].

Recently, both civilian and military leaders have emphasized the "increase in cyber threats and vulnerabilities, making it imperative to act with urgency and purpose to protect the cyber domain from crippling attacks and disruptions." [4]

The threat of degradation or disruption from cyber infiltration, espionage, and theft to militarily and nationally critical information and network systems is real. However, it is possible to be cognizant of the threat and work to close vulnerabilities in the cyber domain and begin hardening of national and DoD network assets while avoiding the pitfalls of threat inflation [5].

To address these threats and vulnerabilities, it is important to have well-trained personnel capable of protecting Navy and DoD networks. The Malicious Activity Simulation Tool (MAST) has been developed incrementally by several Naval Postgraduate School (NPS) students (Taff and Salevski [6], Neff [7], Hammond [8], Longoria [9], Belli [10], and Lowney [11]), as a tool for training Navy and DoD network administrators in the recognition and removal of malware and malicious activities, thus better enabling them to defend DoD networks.

For MAST to achieve its potential as an acceptable assessment and training tool, it must first be shown to

introduce no new vulnerabilities and present no new threats to the environment for which it was designed. This requirement serves as the motivation for this thesis.

A.   PROBLEM STATEMENT

The Malicious Activity Simulation Tool is a software program under development at NPS that mimics the behavior and impact of various malware in a network and creates an environment for training network administrators. Trainees learn to respond to the threats malware presents to their networks and their competence in recognizing and responding to such threats can be assessed. A key element of MAST is its use of Simware – malware mimics that simulate malware behavior (see Definitions, Ch IV). Simware looks and behaves like real malware except that it does not cause the damage that real malware would [6, 8, 10, 11]. Because Simware is safe to use, it can be used for training on live computer networks.

Before fielding MAST on operational networks, thorough testing of the system must be performed in accordance with Navy directives. "At a minimum, new equipment must be laboratory tested to preclude degradation of operational networks during … operations." [12] The same instruction also cites the need for new programs to be capable of interoperation with legacy systems. This thesis describes a methodology for validating both that MAST precludes degradation to operational networks during operations, and that it is capable of interoperation with legacy systems.

3

B.   OBJECTIVES

Following the mantra that "a safe system will do what you want it to, but a secure system will only do what you want it to" [13] this thesis seeks to go beyond the mere functionality testing of MAST. The overarching objective of this thesis is to develop a step-by-step testing procedure, the execution of which will demonstrate that MAST can perform at a level commensurate with current criteria for operating securely on DoD networks.

The MAST Testing Group (see Definitions, Ch II) will face the challenge of clearing a program for operation on a DoD network whose purpose is to simulate activities that are normally screened out in the testing process. [6] Demonstrating that a program induces infection-like behavior in a network during testing is traditionally grounds for failure and removal until said behavior is fixed. In contrast, replicating the conduct of malware is the purpose of MAST. Therefore, in order for it to be considered safe for implementation on an operational network, it must first be demonstrated that MAST will not degrade network operations when it is installed and executed on a cyber test range network. That is, it must be shown that, while it mimics the behavior of malicious software, its activity does not result in the actual behavior of the malware it mimics.

Following demonstrating that MAST can be safely installed and executed on a range, individual Simware modules will be tested. Simware modules are the portions of MAST that specifically simulate malicious activity. The effects of a Simware module can be either visible to the

user, such as slowing of a client's processor, or invisible, such as a port scan or ping [14].

The specified nefarious behavior of an individual Simware module must be shown to be the only malicious activity exhibited while executing that module; accurately replicating or demonstrating only what is expected to be seen.

Finally, operation of the kill switch (see Definitions, Ch IV) must be proven to roll back (see Definitions, Ch IV) the Simware module, resetting the testing network to its previous state and placing MAST in an idle state where it exhibits no negative impact to the environment for which it was designed.

Testing the functionality of MAST, i.e., verifying whether or not the program does indeed perform the functions that it should, is outside the scope of this thesis, as functionality testing has already been completed. The scope herein is limited to demonstrating MAST can interoperate securely on a cyber range test network while performing the functions and operations that it should perform.

C.   ORGANIZATION

The remainder of this document proceeds as follows:

Chapter II provides the reader a brief history of MAST, furnishing information on the evolution from its beginnings as a Malware Mimic (MM) to MAST as it exists today. Chapter II also offers a glimpse into the expected direction of the next wave of students and their plans for MAST in the near future. Further, it provides definitions

to lay the framework for terminology that will be used throughout this document.

An additional feature of Chapter II is the program definition that it provides, so that the historical direction of MAST is reconciled with the direction in which it is now heading.

Chapter III examines the quantitative testing environment and current testing and implementation methods and criteria for new cyber hardware and software programs of record (PORs) in the DoD. This is captured through discussion of DoD cyber ranges, the backbone networks and software suites utilized by the Department of the Navy (DON), and the security system that is currently employed.

Chapter IV describes the step-by-step quantitative testing process for MAST software that satisfies the primary objective set out in this chapter thereby addressing the problem statement.

Chapter V highlights the key contributions of the thesis and provides concluding thoughts of work herein. It also expounds on the expectations of the quantitative testing procedure and looks at future possibilities or areas of study for the Malicious Activity Simulation Tool.

II. BACKGROUND

This chapter provides specific definitions of terms relevant to this research and the quantitative testing process to ensure clarity of intended meaning. Additionally, a brief review of the history of MAST is performed to provide the necessary background information and to consolidate the direction in which MAST proceeds.

A.   DEFINITIONS

For the purpose of clarity, those terms that are necessary to a background understanding of MAST are discussed here.

1.   Testing Group

This term refers to the individuals who will be performing the test of MAST outlined in Chapter IV of this thesis.

2.   Red Team

Red teams are "specially selected groups designed to anticipate and simulate the decision-making and behaviors of potential adversaries." [15] A Red Team is employed to test an organization or entity and determine its resilience against a particular threat or attack. As the term refers to network security testing, Red Teams engage in penetration testing to determine if network administrators utilize proper network hardening measures [15].

3. Penetration Testing

Penetration testing is "a method of actively evaluating the security of an information system or network by simulating an attack from a malicious source." [1]

Penetration testing can include any or all of the following: network reconnaissance/footprinting; network scanning; enumeration; gaining and/or maintaining access to a network [1].

4. Network Hardening

This is the process of eliminating as many security risks to a network as possible in order to reduce the level of vulnerability to threats.

5. Malicious Behavior

Computer network activities whose execution may compromise the confidentiality, integrity, or availability of friendly computer networks and the information they process [1].

Some examples include but are not limited to, network reconnaissance, data exfiltration or modification, and denial of service (DoS).

B. MAST HISTORICAL SUMMARY

This section provides a brief history of MAST from its conception to its current construct.

1. The First Wave: Taff/Salevski

The original groundwork for MAST is laid out in *Malware Mimics for Network Security Assessment*, a thesis by William Taff and Paul Salevski [6].

Taff and Salevski's motivation for this project was to "positively impact national security by improving training for network administrators through the use of a distributed software system." [6] They attempted to replicate what they described as the actions of a "highly trained adversary," a scope that was later refined to focus on malware, such as worms, viruses, and Trojan horses. This replication they sought to accomplish through their MM Software and architecture. They limited their scope to malware – worms, viruses, etc., choosing not to discuss human-centric behavior though they left open the possibility of the "MM-System" expanding to include that wider range of scenarios [6].

a. Purpose:

The purpose of the MM Software was to duplicate Navy Red Team's "effective, realistic, and comprehensive training for network administrators." [6] Taff and Salevski understood that Red Teams do not perform "training" by definition, rather they sought to replicate the training value that Red Team's penetration testing provides for network administrators. The statement, "Exercises [versus] a Red Team are the pinnacle of a unit's training" [6] offers an explanation of the use of the word "training", that is: the context in which the Red Team is attacking, Composite Training Unit Exercise (COMPTUEX), is one of "training".

b. Objective:

Taff and Salevski's objective was to design a network administrator training tool [6] that was:

- Safe enough for use on an operational network, and not constrained to use in the laboratory

- Able to emulate threat behaviors rather than duplicating the threats themselves

- Distributed, allowing for execution from a location geographically separated from the network and network administrators undergoing training

c.   Implementation:

Taff and Salevski devoted Chapter IV of their thesis to describing the creation of the MM-Server and MM-Clients that would become their training tool [6]. They covered sever construction; client construction; communication protocols; and server Graphic User Interface (GUI) design.

They tested the MM on a virtual (VMware) network containing two MM servers and 20 MM client nodes. The tests/experiments had the following objectives:

- Verify that the machines could be controlled [reset] in a timely fashion and that MM-Clients would generate an externally observable network behavior [6]

- Verify the MM-Server and MM-Client software could work on Windows and Linux environments – this was to ensure that the code worked on the common platforms within the DoD and prove the MM-Client's portability between the various Operating Systems (OS) [6]

d.   Results:

The MM Software:

"functioned as it was designed, with feedback between the MM-Server and the MM-Clients. The safety features were adequate in restoring the MM-Clients to their failsafe state during

interruptions in network connections with their respective MM-Sever. Observable network traffic was positively identified [that could] fulfill training and analysis objectives." [6]

The tests determined that "the test platform [was] a suitable testing environment prior to deployment on a live network." [6]

As stated earlier, Taff and Salevski limited the scope of their project to replicating malware – worms, viruses, etc. They included the potential expansion of the MM Software to human-centric behavior as possible follow on work [6].

2. The Second Wave: Neff, Hammond, and Longoria

Justin Neff, James Hammond (who gave the tool its current name) and Ray Longoria next built upon the concepts of Taff and Salevski [6].

a. *Justin Neff*

In his thesis titled "Verification and Validation of the Malicious Activity Simulation Tool (MAST) for Network Administrator Training and Evaluation", Justin Neff sought to "further [Taff and Salevski's] research of a software based 'Malware Mimic' training tool to increase the standardization and availability of network cyber defense training." [7]

Similarly to his predecessors, Neff's motivation for this work was "the increased security of the DoD's computer network assets and ipso facto, the security of the nation as a whole." [7] He aimed to produce this increase in network security through improved training for DoD network administrators.

11

To this end he continued the MM project as it evolved into the Malicious Activity Simulation Tool. His thesis discussed system design advances and modifications, and provided a qualitative analysis of MAST compared against other training methods.
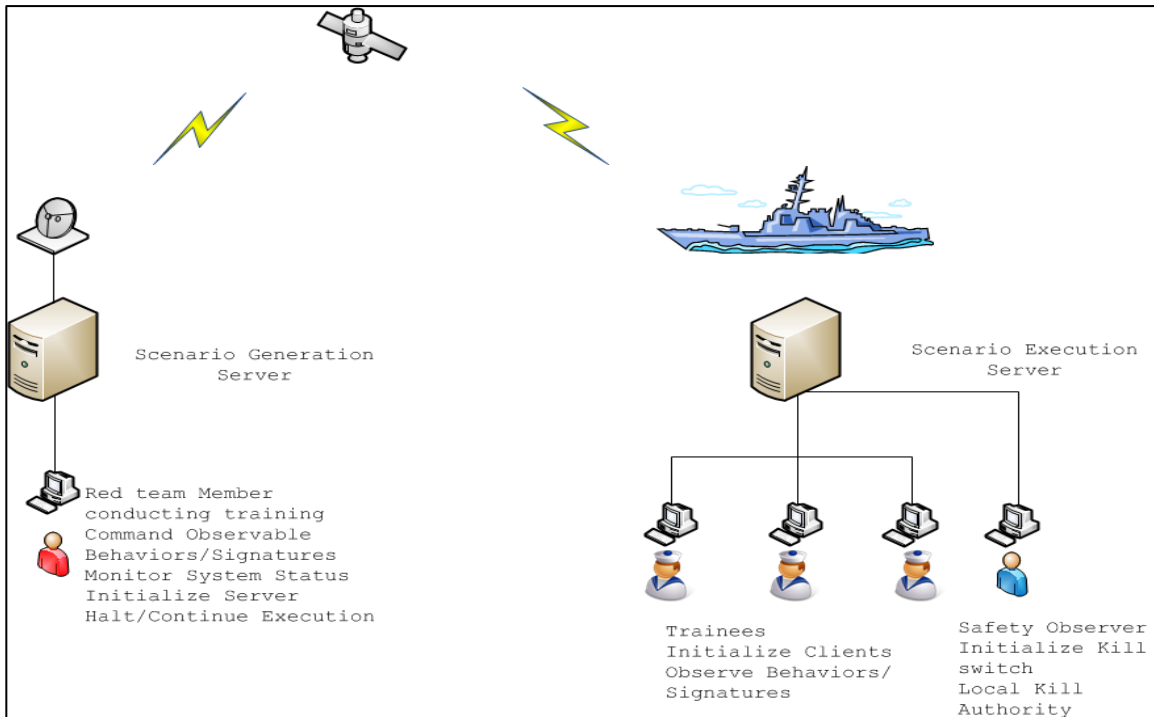
Figure 1.   The MAST Network. From [7].

(1) Design Advances: Neff's work provided insight into the design maturation of MAST. In it, he defined advances that he and James Hammond implemented in the system, server, and host designs. He also discussed the local built-in safety feature, i.e. a software-based "kill switch." [7] The program was still in a virtual environment, but the number of servers (3) and clients (25–30) were increasing as the Virtual Machine (VM) network was expanded to replicate a current DoD network: the Common PC

Operating System Environment onboard a U.S. Navy Guided Missile Cruiser; specifically CG-71.

The local software-based "kill switch" (Figure 1) is configured, Neff described, such that should local conditions warrant the immediate termination of the training scenario, local personnel could end the scenario without having to notify the remote trainer. This would not just halt simulated malicious behavior; it would also immediately "roll back" MAST to its idle state. The network, "as a result of this rollback action, returns to normal operation." [7]

Furthermore, Neff discussed that when a scenario is in progress, should the host lose contact with the remote server, MAST would immediately exit the scenario and roll back to its idle state [7].

(2) Design Modifications: In his thesis, Neff introduced the functionality of MAST as a local training tool, where previously it had been designed solely for remote training. The idea was for this feature to allow MAST to provide a value "similar to NSST" (the Navigation Seamanship Shiphandling Trainer), a program that allows junior officers to improve their navigational proficiency without the expense of getting ships underway. In the case of MAST users, no longer would they have to wait for externally performed penetration testing. Rather, they could "self-test" their network's defenses [7].

Another useful modification was the addition of a database to log the results of a training scenario for comparison with past or future results allowing for "more consistent feedback on training scenarios." [7]

13

(3) Qualitative Analysis: A primary contribution to MAST development offered by Neff was the evaluation of MAST's training utility against that of Red Teams, the Rapid Experience Builder (RaD-X), and the Metasploit Framework, to demonstrate the effectiveness of MAST as a training tool [7]. This he accomplished through the evaluation of ten different training attributes common to the four methods being examined. These attributes included such training concerns as availability, consistency, ease of use of training tool, and training infrastructure.

(4) A Step Further: Toward the end of his work, Neff described what he saw as the "way ahead" for MAST, noting that testing would be required to show that the MAST system "accurately mimics the malware we have implemented in the modules." MAST's scalability would need to be demonstrated, he said, and MAST would then be ready for testing on a cyber range [7].

Notably, Neff also anticipated that in the future as new scenario modules were created to mimic the most current threats facing a network they would "be 'pushed' out to all pertinent network administrators" in the same way that software patches or Information Assurance Vulnerability Alerts (IAVAs) are currently "pushed" to military commands [7].

b. *James Hammond*

James Hammond defined his work as "Malicious Behavior Expansion" and contributed to the MAST project by improving and expanding MAST's architecture (both virtual and actual) [8]. He also expanded the malware behaviors

that MAST would replicate through what he referred to as "client modules" (i.e., Simware modules), and assisted in the creation of some of those modules.

(1) Grouping Malicious Behavior: Hammond defined malicious behavior selection as depicted in Figure 2. In this diagram he refined the scope of the types of malware that MAST would simulate [8].
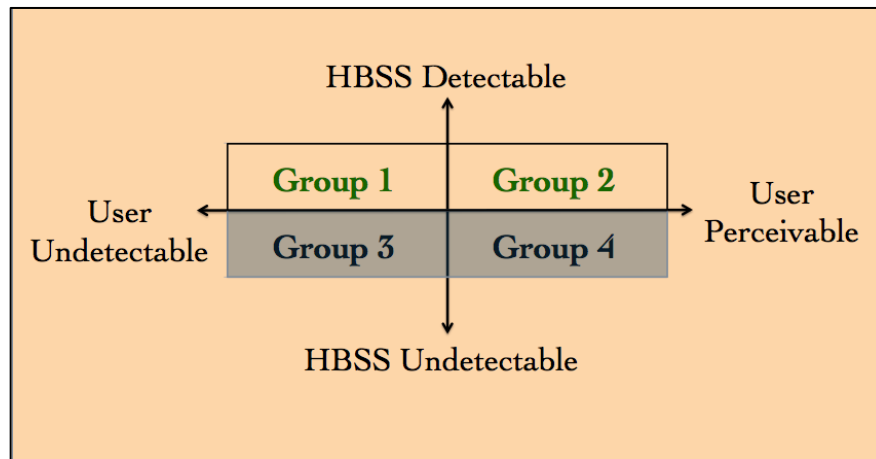
Figure 2.   Malicious Behavior Detection Diagram. From [8].

Group 1 behaviors are Host Based Security System (HBSS) detectable but not user detectable, and are designed:

- Not to impact network users (though users could be impacted by system administrator actions)

- To test proper configuration of HBSS and network devices/sensors and

- To test network administrator's ability to detect and properly respond to malicious activity [8]

Although these behaviors are listed as user undetectable, network administrators should still be capable of detecting their presence and responding.

15

Group 2 behaviors are detectable by HBSS and users and are designed:

- To disrupt network user activity

- To test proper configuration of HBSS and network devices/sensors

- To test network administrator's ability to detect and properly respond to malicious activity and

- To test user's ability to operate in the presence of malicious network activity [8]

(2) Use Cases: Hammond also discussed two sets of "Use Cases." [8] The first "[p]rovide the ability for trained personnel to execute pre-developed cyber training scenarios to support local training objectives, readiness assessments, tests and evaluation." [8]

The second set "[p]rovide the ability for *highly* trained personnel to develop, distribute, and remotely execute complex cyber training scenarios to support readiness assessment; test and evaluation; and cyber tactics, techniques, and procedures (TTP) development" (emphasis in original) [8].

(3) Planned Client Modules: Hammond defined the following planned Simware modules for future work:

- Virus (drop EICAR files randomly across host/hosts)

- Worm propagation (scanning activity and associated network traffic)

- Browser Hijack (local host file modification or other method)

- Switch Overflow (attempt to overflow switch routing table and report results)

16

- Traffic Sniffer (monitor for given parameters and report when met)

- Data Exfiltration (send client module generated data to an off network device; could be expanded to capture actual data and send off network)

- Event Monitor (email attachment execution, cookie creation, etc.)

- Network Reconnaissance (port/protocol scanning, horizontal scanning, raster scanning)

- DoS (e.g., SYN flood) [8]

c. *Ray Longoria Jr.*

Ray Longoria Jr.'s thesis titled "Scalability Assessments for the Malicious Activity Simulation Tool (MAST)" demonstrated the scalability of MAST, specifically "that an exponential increase in clients using MAST did not significantly impact network and system resources." [9]

Part of Longoria's motivation in the MAST project was to rectify DoD network administrator training deficiencies that he identified [9]. To address these shortfalls, MAST, he said, "is designed to simulate and automate some of the training methods conducted by Red Teams" and "One of MAST's key functions is to provide reports on the events surrounding a training scenario." Before moving forward, some clarification is necessary for these statements.

When something is automated it operates with minimal human intervention or independent of external control [16]. It is critical to this project to clarify exactly what is being automated. In this case, the results of each training scenario (the "reports on the events"

Longoria described) will be automatically logged in the Local or Remote Databases (Figure 3). This will provide timely feedback to the trainers and those who are being trained, and will allow them to compare past and present results to demonstrate progress or setbacks. In this way they satisfy Longoria's motivation for improvements to information professional's training.

Original iterations of MAST that were tested in the VM environment were capable of demonstrating and implementing this behavior. However, at this time the degree to which the logging function will be a part of the final MAST product is uncertain.

(1) Research Tests: Longoria's research objectives were to determine the feasibility of loading MAST on a given network and to show the impact MAST had on system and network resources [9]. To accomplish these objectives he performed two tests. The first examined the "impact of deploying MAST from a remote location to a new training network that does not have MAST installed." The second determined "how MAST uses and impacts system and network resources" as the client load was increased.

Longoria performed the bulk of his work and testing on scalability at the same time that Hammond and the system programmers were working to expand MAST's VM network, and therefore their work went hand-in-hand.
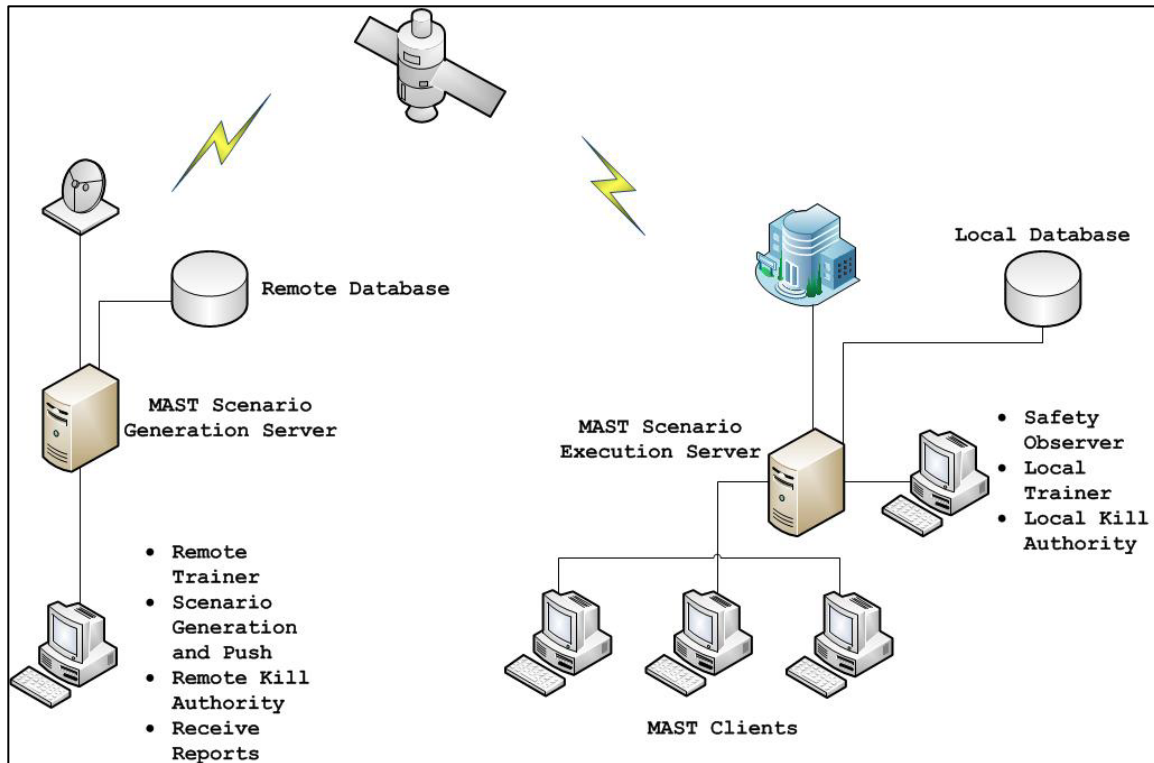
Figure 3.   MAST Network with Databases. From [9].

(2) Results: Longoria's first set of tests demonstrated that "over-the-air (OTA) deployment and local installation is [*sic*] fast and efficient." [9]

The second set of tests verified that system performance did not decrease when client scale was increased:

> "An increase in the number of clients tested did not result in a similar proportional increase in utilization of processing resources. Additionally, an increase in the number of clients and network traffic generated to control those clients resulted in very minimal use of network resources." [9]

Longoria's findings demonstrated "minimal impact on Central Processing Unit (CPU) resources and the capability to serve more clients with ease."

19

An additional finding of Longoria's thesis was in the distribution of feedback and results to the Scenario Execution and Scenario Generation servers, a part of the training improvements mentioned previously. In the VM network, MAST demonstrated the ability to submit feedback and reports with efficiency. Further details, graphs, and specifics of Longoria's findings can be found in his thesis [9].

3. The Third Wave: Hayes and Littlejohn/Makhlouf

As has been the case for some of the previous authors, the motivation for these theses is responding to a need for increased DoD cyber readiness by improving the skill level of DoD network administrators [17]. MAST provides the avenue of approach for addressing this need and we see it as a tool whose implementation will prepare and train network personnel for penetration testing that seeks to identify network security readiness concerns.

The objective of the first thesis is to create a quantitative testing procedure for the MAST Software as it is loaded onto a DoD approved cyber testing range. Littlejohn and Makhlouf will then execute this step-by-step testing process, satisfying the objectives of their joint thesis.

In addition to testing, Littlejohn and Makhlouf will be performing background work to identify assumptions, constraints, and restraints of the MAST Software. An example of this is the oft stated but inaccurate assumption that the purpose of a Red Team is to provide training to tested personnel. The true purpose of a Red Team is to

20

engage in penetration testing to determine the health of a network [18].

Entering a Red Team exercise without preparation and with the expectation of receiving training and guidance from them is akin to showing up to a football game with the hope that the opponent will assist in practice snaps. A penetration test is not the time to receive training; it is game time, and should be approached with the same mentality as General Quarters or any other training exercise in an operational environment.

Preparation for penetration testing must have occurred beforehand to ensure that network administrators are prepared to fight the ship's networks. Ideally this training is based on a simulation of what will be encountered during penetration testing, and this is the training value MAST will provide [18].

THIS PAGE INTENTIONALLY LEFT BLANK

III. TESTING ENVIRONMENT

This chapter examines the quantitative testing environment, current testing and implementation methods, and criteria for cyber programs in the Department of Defense. With a focus on areas pertinent to the Testing Group (see Definitions, Ch II), it includes a look at the various DoD cyber range sites and their standards; the operating platform's backbone networks on which a program would run; and the typical software suite with which the program would interface. Additionally, a brief discussion on Security and Enterprise System Management, notably HBSS, will be included.

A. RANGES

DoD and DON cyber ranges provide fundamental validation and accreditation of systems interfacing with or operating within DoD and DON systems, as well as the training and education of cyberspace personnel. The conceptual backing for cyber ranges that perform these services is established in National Security Presidential Directive 54 and Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) [19].

NSPD-54/HSPD-23 was issued by President George W. Bush in January 2008, and formalizes the Comprehensive National Cybersecurity Initiative (CNCI). The CNCI provides the necessary backing from the top of the Chain-of-Command to mandate the push to a technically proficient force capable of operating in the cyberspace domain with the same level of excellence exhibited in the traditional warfare domains. It institutes a series of continuous efforts to improve

cyberspace security and harden federal government systems to attacks and threats initiated from a cyber vector.

The CNCI focuses on three key areas:

- Establishing a frontline defense against immediate threats by creating and enhancing shared situational awareness of network vulnerabilities and threats, and the ability to act quickly to reduce current vulnerabilities and prevent intrusions

- Defending against the full spectrum of threats by enhancing counterintelligence and increasing supply chain security for key information technologies

- Strengthening the future cyber security environment by expanding cyber education; coordinating and redirecting R&D (research and development) efforts; and working to develop strategies to deter hostile or malicious activity in cyberspace [19]

Meeting the challenges set forth in the CNCI of defending and operating in cyberspace requires expertise in cyber domain operations. Operations in this newest warfare domain require both intellectual knowledge of and the skills and ability to gain access to this battlespace. The tools and weapons needed to gain this knowledge and access are changing at a pace never seen in any of the traditional domains. In this way cyber domain intelligence preparation of the battlespace differs from the domains in which U.S. military branches have become proficient operators.

It is in this capacity that the importance of cyber ranges is realized, as they provide the simulated environments in which tools such as MAST can be developed, tested, improved, and fleet approved.

This section is devoted to a discussion on DoD cyber ranges. As such, individuals with a prior understanding of

cyber ranges may consider skipping to Section B, Shipboard Environments. This discussion is relevant to the quantitative testing process because it provides a single gathering point for information on five specific ranges. Thorough examination of the facilities and capabilities of each site will aid in narrowing the field of DoD cyber testing sites for the Testing Group.

The following is a practical literature review based upon range overviews provided by cyber range supervisors themselves. Looking at the various DoD ranges educates the process of choosing the location at which a program such as MAST would be tested. This section examines functionality testing sites and standards, but stops short of researching the DON and DoD certification and accreditation requirements processes for DoD ranges, as that is outside the scope of this study.

Additionally, there are other DoD ranges available that will not be discussed in this chapter. In the 2012 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) Paper No. 12408, Harwell and Gore of Camber Corporation state that the Air Force has 78 simulators at three locations in Illinois, Mississippi, and Florida – only the range at Scott Air Force Base (AFB), IL will be discussed here. U.S. Strategic Command's (STRATCOM) range, the STRATCOM Cyber Operations Range (SCOR), in Nebraska, will similarly not be discussed. Nor will some cyber training simulators such as the National Guard's Army Guard Enterprise Network Training Simulator (ARGENTS) be discussed here [20]. Rather, this discussion will be

limited to the cyber ranges that the Testing Group are more likely to use in the testing of MAST.

Our selection of cyber ranges includes the following:

- Joint Information Operations Range (JIOR), Suffolk, VA

- Joint Cyber Operations Range/Simulator Training and Exercise (JCOR/SIMTEX), Scott AFB, IL

- Department of Defense Information Assurance Range (DoDIAR), Stafford, VA

- National Cyber Range (NCR), Orlando, FL

- Navy Cyberspace Operations Range (NCOR), Norfolk, VA

Finally, the bulk of the discussion in this section is devoted to the site standards and specifications of the DoD IA Range, the National Cyber Range, and the Navy Cyberspace Operations Range, as these were found to most closely mimic DON network's typical load outs.

1. Joint Information Operations Range (JIOR)

JIOR provides a Joint cyberspace operations testing environment. JIOR is managed from the Joint Staff J7 headquartered in Suffolk, VA. According to their publications, the Range is a "closed-loop, secure, worldwide-distributed network that forms a realistic and relevant live-fire cyberspace environment supporting Combatant Command, Service, and Agency, (CC/S/A) and Test Community training, testing, and experimentation across the Information Operations and Cyberspace mission areas." [21]

The JIOR provides the ability to train and test in a degraded or denied environment on tactical, operational, and strategic levels. Locally delegated authority also allows rapid approval of training and testing events. Most

significantly, JIOR provides connectivity to other DoD and Service's cyber ranges in addition to those of other agencies, National Labs, Industry, and Academia [21].
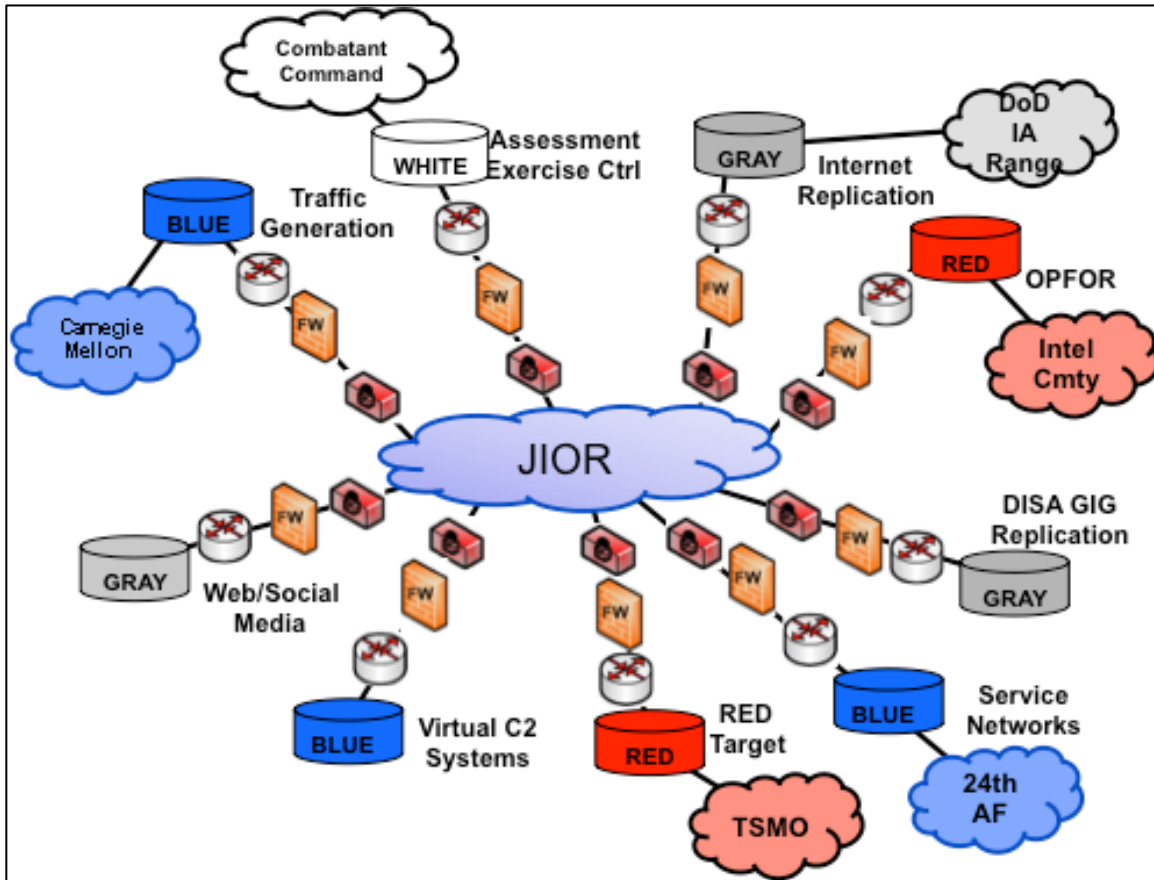
Figure 4.   A Typical JIOR Event Architecture. From [21].

The JIOR is used to test Command and Control (C2) technologies as they traverse the acquisition life cycle. The JIOR network has been accredited and certified by the Defense Intelligence Agency (DIA), and offensive and defensive cyberspace capabilities can be tried in any of seven potential levels of security - from Unclassified to Sensitive Compartmented Information (SCI) [22].

Additional information regarding JIOR facilities and capabilities, as well as methods to gain access to these

can be obtained through the point of contact (POC) provided in the Appendix.

2. Joint Cyber Operations Range/U.S. Air Force Simulator Training and Exercise (JCOR/SIMTEX)

JCOR/SIMTEX is the environment at Scott AFB, IL, run by Camber Corporation on behalf of the Air Force. JCOR is a consortium of users that utilize Camber's cyber simulators to conduct training (both formal and operational) along with participating in Joint, Service and government exercises. This consortium currently includes the Air Force, Navy, National Guard, and USSTRATCOM as full-time members [22, 23].

JCOR is capable of being distributed via previously discussed JIOR connectivity. The JCOR environment is typically utilized as an Air Force specific training environment, but can be adapted for use by other entities [22, 23].

For the Navy, JCOR's simulator can represent afloat units and afloat Navy Operations Centers (NOCs) with sensor feeds representing Navy Cyber Defense Operations Command (NCDOC). This representation is housed at the Navy Information Operations Command (NIOC) in Norfolk, and managed by the 10TH FLEET N72. The Navy currently uses the simulator for cyber exercises; operational training, such as the Computer Network Team Trainer (CNTT); tool development for Navy Red Teams; HBSS training; and other miscellaneous uses [22, 23].

In 2012, the Camber Corp. provided the simulators with traffic and attack generation for the National Collegiate Cyber Defense Competition Finals in San Antonio, TX and

will take part in the 2013 competition as well. However, the simulators are normally used for USAF cyber personnel training and Computer Network Defense in Depth courses of instruction.

Each simulator environment is designed to the specifications of the users' operational environment and is scalable and interoperable. They also have both classified and unclassified capabilities depending on the environment and the requirements they support [22, 23].

Additional information regarding JCOR facilities and capabilities, as well as methods to gain access to these can be obtained through the POC provided in the Appendix.

3. Department of Defense Information Assurance Range (DoDIAR)

DoDIAR is located near Marine Corps Base, Quantico in Stafford, VA. The Defense Information Systems Agency (DISA) provides program sponsorship for DoDIAR. Headquarters Marine Corps (HQMC) Command, Control, Communications, and Computers (C4) provides program management, Certification and Accreditation (C&A), program outreach, and contract support for the Range [22].

HQMC C4, in partnership with DISA Program Executive Office for Mission Assurance (PEO-MA) and the Office of the Under Secretary of Defense, has also enabled the DoDIAR to support the training, exercise, and test and evaluation communities in the pursuit of the following stated goals: to exercise cyber warriors; to test and evaluate new capabilities; and to train network defenders [22, 24].

DoDIAR was created and funded on the basis of the CNCI and was commissioned to develop and host a realistic DoD GIG. This fully accredited environment provides "maneuver areas where Cyber Warriors can conduct cyber training, testing, and exercises in an environment identical to their daily field of battle." [25]

DoDIAR is reflective of GIG Information Assurance/Computer Network Defense (IA/CND) capabilities and network services and provides a Joint-Services environment for cyber exercises, Computer Network Defense Service Provider (CNDSP) training, and testing and evaluation of CND products and operational TTPs [25].

There are no actual classes or cyber exercises performed by Range personnel; rather, that is a customer function that they facilitate. They maintain the network spaces required to execute cyber tests and training [25].

DoDIAR normally provides fee-based access, however its services would be available to the Testing Group at no cost, as is the case for all DoD personnel. Access to the Range can be achieved either remotely (using a Remote Boundary Suite [RBS] via a secure Virtual Private Network [VPN] tunnel) or locally in Stafford Virginia [24].

The IA Range may be operated in a standalone simulator mode or can interface and interoperate with other ranges provided by CC/S/A. Communications are secure between all parts of the IA Range and the CC/S/A virtual enclaves. Range traffic is routed on a closed network environment. This prevents accidental leakage of classified, proprietary, or potentially hazardous entities to operational networks [22, 24].

DoDIAR currently operates at the "Unclassified" level. In July of 2012 the Range built an identical environment to the one in Figure 5 that will be capable of operations at the Secret level. It is the same unclassified GIG, but in an environment where Secret TTPs can be developed and practiced, Secret defense or attack tools can be incorporated, or Secret scenarios can be executed. This Secret environment incorporates a Secure Internet Protocol Router Network (SIPRNet) backbone that rides on the GIG. In fiscal year (FY) 13, the Cyber Range will have an identical environment that will operate at the Top Secret/Sensitive Compartmented Information (TS/SCI) level with a SIPR and Joint Worldwide Intelligence Communications System (JWICS) network riding on the GIG [24].

According to the DISA Security Technical Implementation Guide (STIG), the IA Range is required to perform as a "closed network environment," meaning it is forbidden from connecting to any live network because of the concerns stated previously. The DISA STIG identifies these types of environments as "Zone D enclaves." These enclaves may be closed but are permitted to connect to other Zone D environments, and DoDIAR was designed to perform these connections. In this way the Range can provide customers with closed labs access to its virtual DoD GIG as well as the enterprise services DISA provides [24].

Additional information regarding DoDIAR facilities and capabilities, as well as methods to gain access to these can be obtained through the POCs provided in the Appendix.
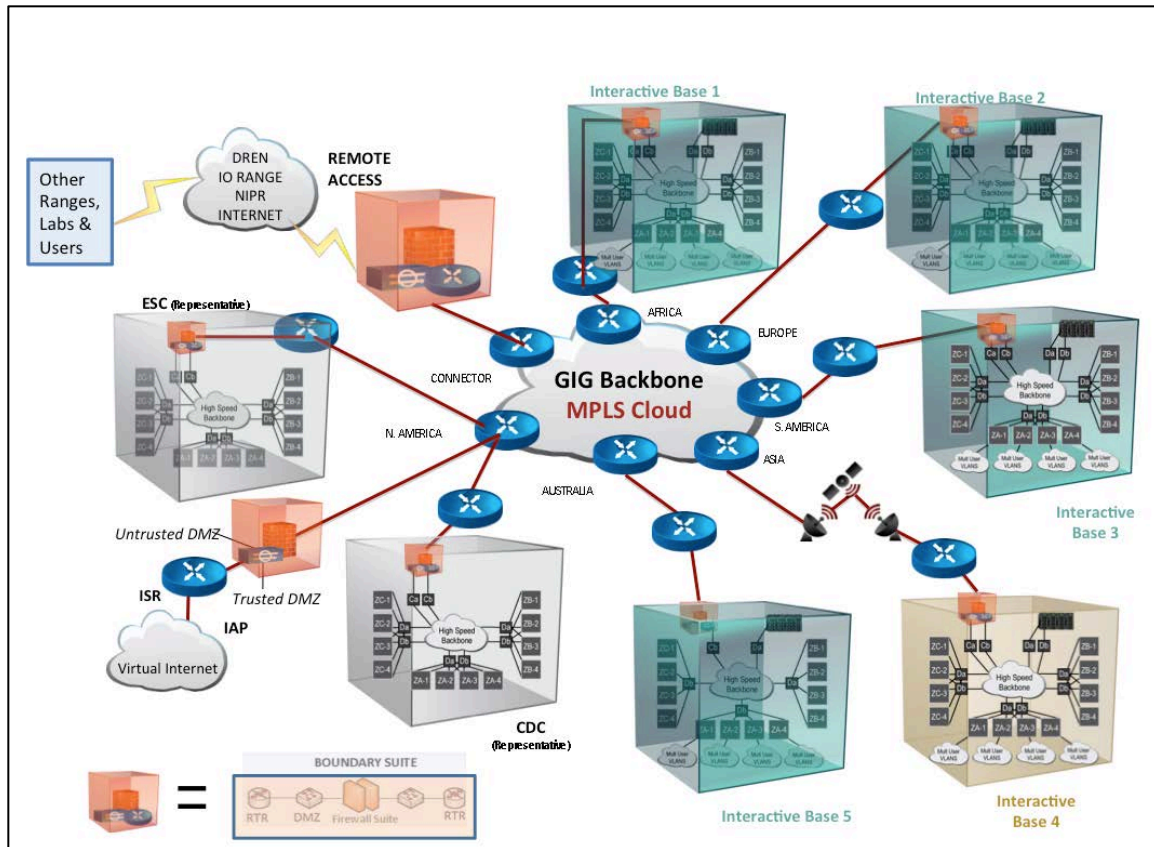
Figure 5.   DoD IA Range Topology. From [24].

a.   *DoD IA Range Topology Analysis:*

A general, abbreviated description of the DoD IA Range's topology as it is depicted in Figure 5 follows, taken from the original figure in Range documentation:

> "The IAR provides a Multi Protocol Label Switching (MPLS) cloud comprised of [six] Provider Edge (PE) routers representative of the DISA GIG. Downstream from [five] of the PE routers are interactive bases that are composed of the standard Cisco design model for networks (Core Layer, Distribution Layer, Access Layer) with [eight] disparate distribution zones (user zones) to simulate a given base's cable plant, as well as a server farm hosting the following services: email (MS Exchange), Active Directory, Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), file share, and print services.

Each user zone within a base can support 10 Virtual Local Area Networks (VLAN) comprised of 254 users per VLAN. Downstream from the [six]th PE router are [two] facilities for hosting specialized applications similar to the functionality of DISA Defense Enterprise Computing Center (DECC) and Community Data Center (CDC). Currently, the IAR CDC hosts both ArcSight and SourceFire." [24]

4. The National Cyber Range (NCR)

NCR utilizes a prototype built by Lockheed Martin, and is located at the Lockheed Martin Facility in Orlando, FL. CNCI provides funding for the NCR initiative that was run by Defense Advanced Research Projects Agency (DARPA) until Oct 2012, when it transitioned to the Office of the Secretary of Defense, Acquisition, Technology, and Logistics (OSD/AT&L) Test Resource Management Center to determine its operational relevance and capabilities to rapidly provision large-scale environments representative of DoD Networks. At the time of the NCR Program Overview the size of the NCR range was sufficient to emulate a DOD network of 3000 users [22, 26].

The objective of the NCR is to provide a testing environment that supports the CNCI's key focuses (discussed earlier) through supporting the development of advanced technologies, with the goal of creating a secure representation of DoD and industry networks. This would improve the certification process for cyber technologies [26].

According to Lockheed Martin's 2012 Program Overview for NCR, the primary objectives of the Range are to "enable multiple, independent, simultaneous experiments from the Unclassified to TS/SCI level at the same time; enable rapid

construction of experiments; and rapid sanitization and reuse of assets after experiments' conclusion." [26]

Lockheed Martin hopes to achieve these objectives by enabling a "5-10 fold reduction in the time (one to six months reduced to three to 30 days) and cost ($1-5 million cut to $50,000 to $500,000) for cyber testing and research." [26]

a. NCR Key Features

The prototype that Lockheed Martin designed and built for NCR provides a number of key features, some of which would prove useful to the Testing Group should they chose to utilize NCR as a test site. The first of these is simple design tools to enable users to quickly design the network topology and specific tests for a cyber experiment. These tools can also be run at the users' location, increasing accessibility to cyber testing [26].

The second key feature discussed in the 2012 Program Overview is the "employment of hardware and software tools that automate the process of building out and configuring NCR for a cyber test consisting of thousands of physical machines." This would allow for a reduction in the time that is spent configuring the range for a large-scale test from months to hours [26].

The third key feature is an "automated range sanitization process to completely reset the range after testing for reuse at any classification level." This would allow for the introduction and testing of new code without endangering the range itself [26].

Last, employing a security architecture that allows multiple experiments to run on the range simultaneously with different classification levels would again allow for maximum range utilization. NCR is accredited for TS/SAP, and was undergoing SCI accreditation testing at the time of this composition. Range users must possess a minimum clearance of Secret, and Privileged Users will require access to the highest clearance level of data processed [26].
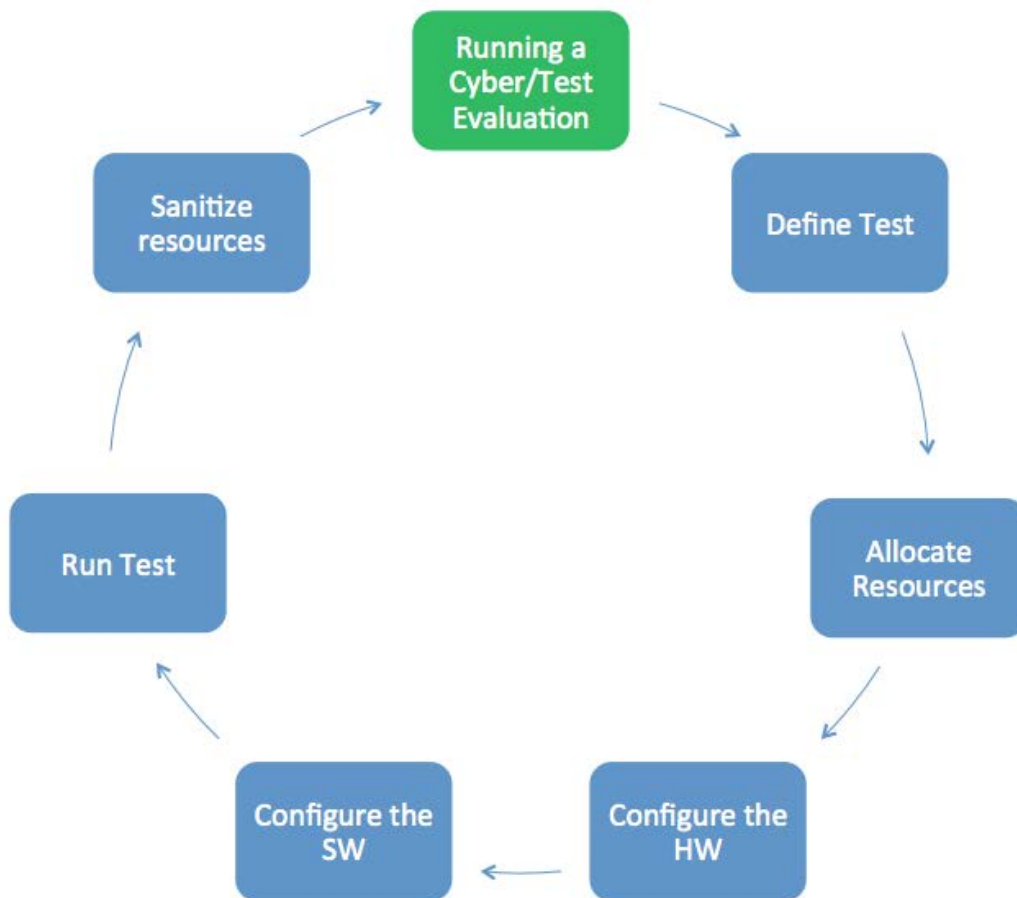
Figure 6.   The NCR Automated Cyber Test Process Cycle. From [26].

b. *The NCR Automated Cyber Test Process Cycle*

NCR has a seven-step, automated cyber test process that would guide the Testing Group through its cyber and test evaluations. The process starts with a common pool of hardware (HW) and software (SW) resources and cyber tool sets. The follow-on steps as described by Range documents are:

Step 1: Define Test – Utilize test specific tools to define end to end aspects of test

Step 2: Allocate Resources – Automated scheduler determines what resources from the pool are needed and allocates them to test

Step 3: Configure HW – Range Configuration Tools automatically wire HW to the appropriate configuration

Step 4: Configure SW – Range Configuration Tools automatically configure and verify the SW needed to run test

Step 5: Run Test – Test team validates environment, installs System Under Test and runs test/collects data using toolset

Step 6: Sanitize Resources – Sanitize HW and "virtually" put HW/SW resources back in pool

The completion of Step 6 results in a full circle to the starting point where previously run cyber/test evaluations can be re-evaluated, or entirely new ones can be processed in the same cycle [26].

c.   NCR Test Configurations:

The testing configurations that are possible at NCR include but are not limited to: a standard military NOC, a small business network, a university network, or a home network infected with malware. Example test vectors include scans, Malware Injection (such as Metasploit or Repository), or command line actions [26].

Additional information regarding the NCR's facilities and capabilities, as well as methods to gain access to these can be obtained through the POC provided in the Appendix.

5.   Navy Cyberspace Operations Range (NCOR)

NCOR is located at the Navy Information Operations Center (NIOC) in Norfolk, VA. The Navy currently uses the simulator there for cyber exercises; operational training, such as the CNTT; tool development for Navy Red Teams; and HBSS training, among others [27].

Camber Corporation's NCOR Overview provides a list of the Range's capabilities. In addition to cyber exercises, operational assessments, and tools and application development, the Range also provides penetration testing, competition hosting, mission rehearsals, network validations, certification and accreditation support, and training – both on-site and distance learning when remote connectivity is available [27].

a.   System Description

The NCOR Overview gives a general definition of this Range as "a suite of equipment that creates a

simulation network; a cyber exercise, assessment, and training simulator/environment, as well as an application development and testing network." [27]

NCOR is an isolated computing and networking environment that replicates realistic network enclaves where the Testing Group could test MAST without endangering operational or production networks. It is also noteworthy that NCOR is currently used to test commercial and custom developed security applications, such as HBSS and Navy Red and Blue Team toolkits, under varied networking configurations [27].

NCOR can operate as a stand-alone range and, because it uses standard protocols, it can also be connected with other ranges via isolated range WANs, such as the JIOR or DoDIAR (see Ch III.A.1 and .3), to network equipment in order to form larger environments. NCOR's expanded operating architecture is centered on the JCOR WAN (see Ch III.A.2) [27].
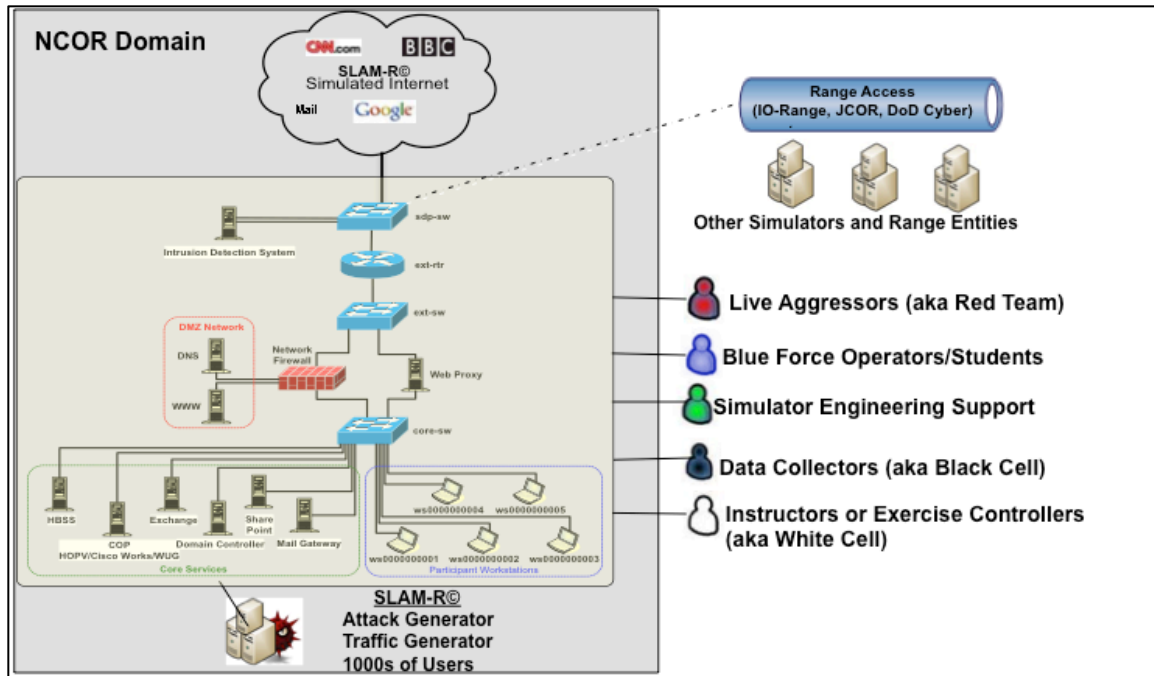
Figure 7.   NCOR's Conceptual Network. From [27].

b.   The NCOR Operating Environment

NCOR consists of servers, routers, switches, and security appliances configured to simulate Navy afloat networks. Ship-to-Shore IP data flow and packet forwarding has been replicated at the Range, and the hardware and software components used are industry standard items that are commonly found within the fleet (e.g. Cisco routers, Alcatel switches, McAfee Intrushield, Sidewinder Firewall, Windows 2003/2008 servers) [27].

Significantly to the MAST Testing Group, the Cyber Range has been pre-loaded with a shipboard-configured Common PC Operating System Environment 3.0.1 (See Ch III.B.1) domain with an integrated HBSS solution. Additionally, "NCOR's exercise servers and workstations are virtualized within a VMWare ESXi 5.0 framework.   This

39

virtualization enables the simulation environment to be rapidly reset after training events." [27]

Additional information regarding the Navy Cyber Operation Range's facilities and capabilities, as well as methods to gain access to these can be obtained through the POCs provided in the Appendix.

6.   Summary:

This section has furnished an overview of the capabilities and facilities of five DoD ranges: JCOR, JIOR, DoDIAR, NCR, and NCOR. This serves the purpose of providing a single gathering point for information on these varied ranges. Additionally it provides the Testing Group with the base of information necessary to choose a range for the quantitative testing process.

The following section is devoted to a discussion on Navy Shipboard Environments, specifically the Common PC Operating System Environment (COMPOSE) and the Consolidated Afloat Networks and Enterprise Services (CANES). As such, individuals with a prior understanding of these may consider skipping to Section C, Shore Environments.

B.   SHIPBOARD ENVIRONMENTS: COMPOSE/CANES

A discussion of Shipboard Environments is relevant to the quantitative testing process because the Testing Group will need to prove that MAST is capable of interfacing with legacy and current versions of COMPOSE if it is to become a useful shipboard network administrator training tool. Tolerance for legacy architecture and programs is imperative because of the prevalence of older, sometimes outdated systems and programs. This requirement was

reemphasized as recently as February 2013, in Operational Navy Instruction (OPNAVINST) 9410.5C, the Navy Tactical C4ISR Interoperability Procedural Interface Standards Requirements, Certification, and Testing [12].

As for CANES, its installation is scheduled to be complete on 192 platforms in the next five years [28]. It therefore becomes equally imperative for MAST to be capable of interoperations with CANES in order for it to efficiently operate on all shipboard platforms.

This section provides an examination of COMPOSE and CANES to demonstrate the importance of interoperations with each, and to prepare the Testing Group for operating in each Environment.

The Department of the Navy's Chief Information Officer (DON CIO) is responsible for oversight and management of Naval networks both ashore and afloat. This includes developing strategy for the Naval Networking Environment (NNE); participating in acquisition milestone gate reviews; and ensuring interoperability, developing policy and providing compliance oversight for the COMPOSE and CANES Environments, among others [29, 30].

COMPOSE and CANES fall under the cognizance of the Navy's Tactical Networks Program Office, Program Manager, Warfare (PMW) 160, located in San Diego, CA, and reports to the Navy's Program Executive Office for Command, Control, Communications, Computers and Intelligence (PEO C4I) [31].

The Space and Naval Warfare Systems Command (SPAWAR, the Navy's Information Dominance systems command) website states that PMW 160 provides affordable, interoperable, and

secure net-centric enterprise capabilities to the Navy. PMW 160 also provides the network services used by many shipboard tactical and business applications and systems, a common network infrastructure across security domains, and supports cross-domain and coalition operations [32].

COMPOSE and CANES are Shipboard Environments similar to the OS of a computer. COMPOSE is common throughout the fleet and provides a Microsoft© Windows™ OS for the server and clients, as well as the necessary software required to carry out standard Navy business [29]. CANES is the technical and infrastructure consolidation of existing, separately-managed, afloat networks. Navy networks began transition to CANES in the first quarter of FY 2013 [28].

1.   The Common PC Operating System Environment (COMPOSE) Program

COMPOSE provides a common office-automation environment for the conduct of standard Navy business, such as maintenance scheduling and supply ordering. Fielding for COMPOSE first began in April 2004. COMPOSE was able to offer a much improved architecture over its predecessor (GOTS-Delta) by utilizing a modular commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) software bundle that delivered directory services, e-mail, web acceleration, office automation applications, and antivirus software [29, 33].

According to DON CIO, COMPOSE provided two major benefits to the Navy when it was implemented: security and cost savings. First, the introduction of Windows™ 2000 Server architecture into the fleet came "as part of PMW 160's solution to the risk posed by Windows™ NT End-of-Life

(EOL)." Second, "[it] marked the beginning of a steady and deliberate progression away from GOTS toward COTS solutions." COMPOSE services also came in a secure software bundle that aligned to the latest DISA standards and guidelines [29, 33].

The COMPOSE architecture provided these streamlined upgrades, services, and software to the Integrated Shipboard Network System (ISNS), Combined Enterprise Regional Information Exchange System (CENTRIXS), SCI networks, and Submarine Local Area Network (SubLAN). COMPOSE was also utilized as a core component for such PORs and systems as: Global Command and Control System-Maritime (GCCS-M), Naval Tactical Command Support System (NTCSS), Distributed Common Ground System – Navy (DCGS-N), and the Navy's latest Guided Missile Destroyer, DDG-1000 [29, 33].

Additionally, (and of particular importance to the Testing Group) older versions of Windows™ clients were supported in order to provide compatibility for legacy applications that had not yet transitioned to more recent versions of Windows™ supported by subsequent COMPOSE upgrades. A tolerance for legacy architecture and programs is imperative for any system or program seeking implementation in the fleet because of the prevalence of older, sometimes outdated, systems and programs. [34].

Table 1 shows the basic implementation and EOL timeline, the OS version for both server and workstation, and the fielded networks for GOTS-Delta and the initial and follow-on versions of COMPOSE.

Version	End-of-Life	Server OS	Workstation OS	Fielding	Notes
GOTS-Delta	31-Dec-04	Windows NT	Windows NT	1st generation of Fleet baseline SW	
COMPOSE 2.0.3	13-Jul-10	Windows Server 2000	Windows 2000 Pro	ISNS, SubLAN, and SCI networks	Windows 2000 Support Agreement in place until 13 July 2011
COMPOSE 3.0.0/3.0.1	8-Apr-14	Windows Server 2003 Standard	Windows XP Pro with support for 2000 Pro	ISNS and CENTRIXS	SCI and SubLAN began fielding in FY09
COMPOSE 3.5.0	8-Apr-14	Windows Server 2003 Standard R2	Windows XP Pro with support for 2000 Pro	ISNS as Mod 3 – initial install Q2FY09. SCI as Prod Mod – initial install FY10	Office 2007 and IE7 & Microsoft SMS and Image Deployment
COMPOSE 4.0.0	11-Apr-17	Windows Server 2008 Standard (64-bit)	Windows 7 (32- and 64-bit)	Brought Microsoft SCCM* Server, Updated Image Deployment & IE8	Support current POR network transition to CANES

Table 1.   COMPOSE Version Implementations and Operating Systems. After [33].

2. Consolidated Afloat Networks and Enterprise Services (CANES)

CANES is a network environment developed by Lockheed Martin, MS2 Tactical Systems in San Diego, CA, and Northrop Grumman Space and Mission Systems Corporation in Reston, VA. CANES has been designated as the technology replacement for the current afloat networks and is to become the Navy's core-computing infrastructure [35]. According to Jane's [28], as of December 2012, installation had begun on the first of 10 CANES systems planned for fiscal year 2013. The Navy began the initial work of removing and replacing the legacy hardware and cabling associated with the previous network system aboard USS *Milius* (DDG 69). The installation was expected to take 18 weeks, and should be completed on 192 platforms in the next five years [28].

CANES is the technical and infrastructure consolidation of current afloat networks and was designed to provide the necessary infrastructure for applications, systems, and services for shipboard operations. CANES combined several separately managed afloat networks such as ISNS, CENTRIXS-Maritime (CENTRIXS-M), and SCI Networks. These legacy afloat network designs reached EOL starting in FY 2012, and CANES has been replacing them as they become unaffordable and obsolete [35, 36].

A large number of applications are currently hosted on the ISNS Early Adopter Network preceding CANES, and CANES will host even more. It is designed to operate unattended, with network management tools continuously monitoring key system parameters and services [37]. The Navy hopes that CANES will bring standardization across the fleet by

reducing the variants of networks currently in use. This will enable information technology (IT) sailors to engage in ship-to-ship transfers and run virtually the same network, resulting in a consistency that has been previously lacking on afloat platforms.

Through this transition, the Navy will also gain inherent IA and security capabilities that were not built into legacy networks but were added as an afterthought when cyber security risks arose [28].

Commander, Operational Test and Evaluation Force's (COMOPTEVFOR) Integrated Evaluation Framework (IEF) [38] describes CANES as "the hardware, OSs, and end user devices within four distinct security enclaves that provides Multilevel Security (MLS) network access through Cross Domain Solutions (CDS)" (see Figure 8) for all basic network services to a wide variety of Navy operational platforms. It goes on to say: "CANES implements a Common Computing Environment (CCE) for application hosting that is intended to provide enough server capacity to support shipboard computing requirements and all business, intelligence, and warfighting POR systems."

Regarding those POR systems, the U.S Navy Program Guide 2012 states that "approximately 36 hosted applications and systems… require CANES infrastructure in order to operate in the tactical environment… [and] are dependent on the CANES [CCE] to field, host, and sustain their capability because they no longer provide their own hardware." [35]

It is also noteworthy that CANES plans to provide functionality currently provided in elements of Afloat

Computer Network Defense (ACND). CANES will field on rolling four-year hardware and two-year software baselines and will achieve full deployment by FY 2023 [35].
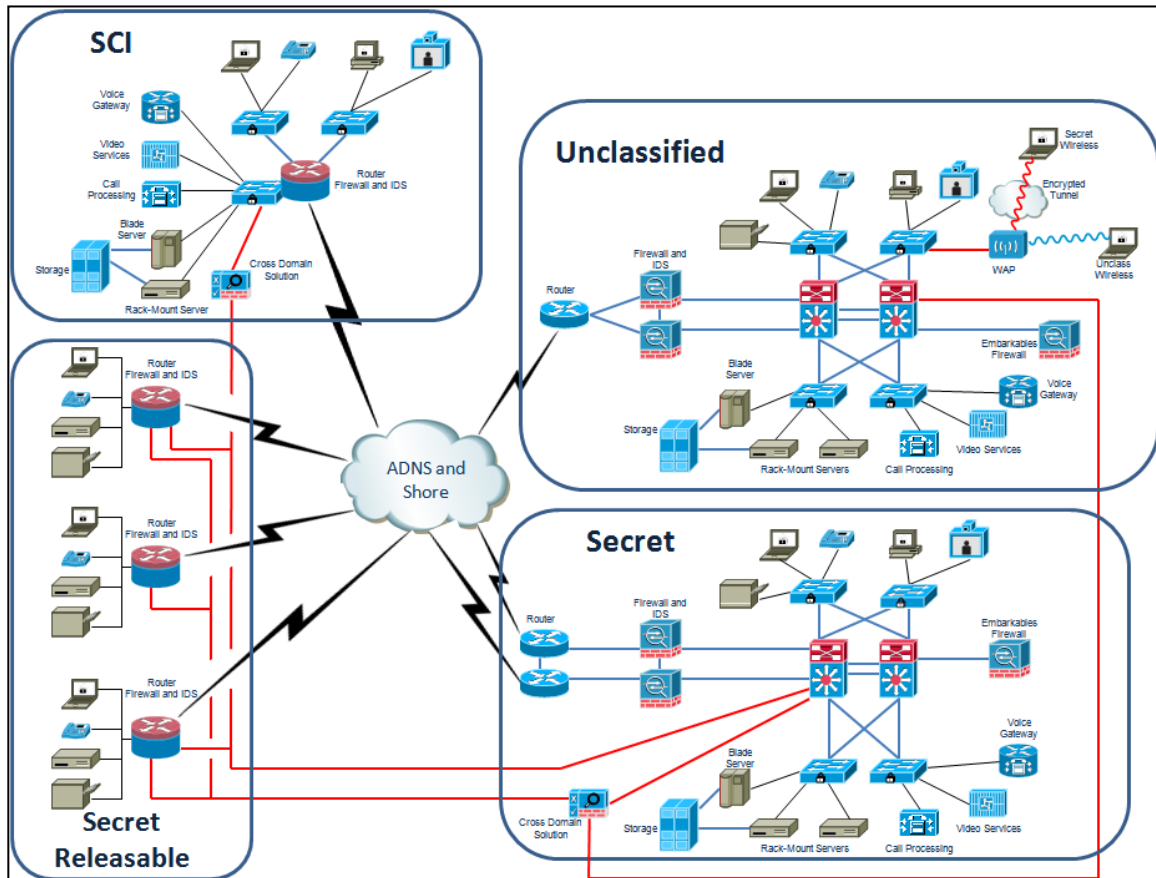

Figure 8.   CANES Topology. From [37].

a.   CANES Topology

Each of the four CANES security enclaves hosts a separate system of systems. Common characteristics include shipboard support systems, Automated Digital Network System (ADNS), Navigation Sensor System Interface (NAVSSI), locally and remotely hosted applications, connections to the GIG, and remotely accessible services [38].

3. Summary

A program tool such as MAST must be capable of interfacing with COMPOSE and CANES if it is to function on afloat operating platforms. To wit, this section furnished basic information on these shipboard environments to the Testing Group to facilitate their understanding and knowledge of them.

The following section introduces the DON shore environments, specifically the Navy Marine Corps Intranet (NMCI), the OCONUS Navy Enterprise Network (ONE-Net), and the Next Generation Enterprise Network (NGEN). Again, individuals with a prior understanding of these may consider moving ahead to Section D, Security and Enterprise System Management.

C.   SHORE ENVIRONMENTS: NAVAL ENTERPRISE NETWORKS (NEN)

This discussion is relevant to the quantitative testing process because working within NMCI, ONE-Net, or NGEN is a daily and necessary part of Navy network operations. This section provides some general information and overall system parameters to facilitate the understanding of these environments and operations in them.

As mentioned in the previous section, DON CIO is responsible for oversight and management of Naval networks. This includes developing strategy for the NEN, both ship- and shore-based, and ensuring interoperability, developing policy and providing compliance oversight [30].

NEN is part of the DON Program Executive Office for Enterprise Information Systems (PEO-EIS). Established in the Spring of 2006, the PEO ensures that programs maximize

value to the Navy by balancing cost with the capability delivered to the end user. PEO-EIS manages a portfolio of enterprise-wide IT programs designed to enable common business processes and provide standard IT capabilities to sailors and Marines and their support systems [39].

The NEN Program Office (PMW 205) was established in February 2011 to "manage the acquisition life cycle of the Navy's enterprise-wide IT networks." [39] PMW 205 is responsible for the three PORs that will be discussed in this section:

The Navy Marine Corps Intranet (NMCI) is the DON shore-based enterprise network in the continental United States and Hawaii, providing "a single integrated, secure IT environment for reliable, stable information transfer." [39]

OCONUS Navy Enterprise Network (ONE-Net) "evolved from the Base Level Infrastructure Information (BLII) Modernization Program in 2005. ONE-Net provides secure, seamless and global computer connectivity for the DON outside the continental U.S. (and Hawaii)." [39]

NEN also provides program management of the NMCI Continuity of Services Contract (CoSC), a contract that extends the life of NMCI and ONE-Net and maintains network services during the Department's transition to NGEN [39].

Next Generation Enterprise Network (NGEN) "represents the continuous evolution of [DON] enterprise networks and will provide secure, net-centric data and services to the Navy and Marine Corps personnel." [39]

1. NMCI – Navy Marine Corps Intranet

Implemented in 2001, the NMCI architecture replaced the Information Technology for the 21st Century (IT-21) and Marine Corps Tactical Network (MCTN) architectures. This was in response to a 1999 SECNAV directive to DON CIO to integrate the Navy and Marine Corps networks [40].

According to SPAWAR's website, NMCI "currently represents about 70 percent of all DON IT operations and is second only to the Internet in size." It goes on to say that NMCI "revolutionized the way the DON operated in cyberspace in both classified and unclassified environments." [41, 42]

Similar to the primary benefit of COMPOSE, NMCI increased standardization in Navy and Marine Corps network operations. It also increased "data security, technical support and real-time communications" through the implementation of common hardware, software and OSs. These improvements resulted in "increased productivity, greater interoperability, and enhanced [IA] security." [40]

The CIO claims that NMCI significantly increased network security over its predecessors, thwarting thousands of unclassified intrusion attempts each month, blocking millions of spam messages, and detecting viruses [43]. A few of the primary reasons for this improved security were "eliminating points of entry; switching to multi-layered defense; and allowing for fielding of public key infrastructure (PKI) and smart cards." [44]

a. General Statistics:

According to the PEO OIS [41], NMCI currently has:

- More than 810,000 users

- 384,000 workstations and laptops in more than 3,000 locations

- More than 3.4 terabytes of data transported and 124 million browser transactions per day

- 38 classified and unclassified server farms

- 28 micro-server farms

- Four NOCs that provide redundancy and security for network information

b. Continuity of Services Contract (CoSC)

The NMCI contract expired on 30 September 2010. Just prior to expiration, the DON awarded the NMCI CoSC to Hewlett-Packard. NMCI CoSC provides a bridge between NMCI and NGEN and "ensures the seamless connectivity and security of NMCI." [48]

According to SPAWAR [41], NMCI CoSC:

- "Provides IT services during the transition from the NMCI contract to the proposed [NGEN] solution

- "Increases governmental technical authority and ownership over critical network operations and infrastructure

- "Allows the DON to competitively procure network services that support enterprise IT goals, encouraging greater participation from the IT industry while ensuring continuity of services at the close of the NMCI contract." [40]

2. OCONUS Navy Enterprise Network (ONE-Net)

ONE-Net evolved from the BLII Modernization Program in 2005. It was a Navy-wide initiative to install a standardized, secure, global IT infrastructure to OCONUS Navy installations. ONE-Net was based on the NMCI

architecture and was designed to be interoperable with IT-21, NMCI, and the GIG [39].

Oversight of ONE-Net is currently part of the NEN Program Office that manages the acquisition life-cycle of DON enterprise-wide IT networks [39].

ONE-Net delivered "comprehensive, end-to-end information and telecommunication services to OCONUS Navy shore commands by using a common computing environment for both the Non-secure Internet Protocol Router Network (NIPRNet) and Secure Internet Protocol Router Network (SIPRNet)." [39] It also standardized hardware and software and increased IA and network security, providing users with "access to an OCONUS e-mail directory, a standard e-mail address, and increased SIPRNET availability and remote access." [45]

ONE-Net is currently designated as government-owned and -operated and will continue to be so "until the network transitions to NGEN and adopts the NGEN operating model and support structure." [46]

3.   Next Generation Enterprise Network (NGEN)

NGEN represents the next evolution of DON enterprise networks and will supply secure IT infrastructure and services to the Navy and Marine Corps. NGEN will serve as the DON's replacement for NMCI and ONE-Net, and will provide enterprise network services, namely: secure, standardized, end-to-end, shore-based information technology capability for voice, video and data communications [41, 47].

A primary benefit of the NGEN upgrade to NMCI will be the inclusion of IA enhancements capable of meeting evolving security requirements. SPAWAR's years of experience with NMCI will guide NGEN's implementation process. The NGEN Acquisition Strategy also imitated the segmented approach recommended by Fortune 500 CIO best practices for IT, "acquiring IT services via the competitive award of multiple contracts for local transport, hardware, software and enterprise services." [40]

DON CIO is looking to NGEN to provide the Navy and Marine Corps improved access to the information and services that are necessary to accomplish the military's mission in a Cyber Age. It also expects NGEN to provide a robust information system that will keep up with the pace of technological improvements [43].

NGEN has begun the transition and implementation process for the Marine Corps and anticipates completion by May 2013. Transition of Navy networks will follow and is scheduled to be concluded by April 2014 [47].

DON CIO anticipates that NGEN:

- "Will provide a 24/7 enterprise level service, with four NOCs and three enterprise service desks.

- "Will be deployed to approximately 400,000 workstations and laptops while creating nearly 800,000 NGEN user accounts and serving more than 3,000 locations in the continental United States, Hawaii, Alaska and Okinawa." [47]

4.   Summary

This   section   provided   information   on   DoN   shore environments for the purpose of shedding light on their functionality, or in the case of NGEN, the expected system functionality.

A program tool such as MAST must be capable of interoperating with NMCI, ONE-Net, and soon NGEN in order to be operational on shore facilities. For this reason, this   section   furnished   basic   information   on   these environments to the Testing Group to facilitate their understanding and knowledge of them.

The   following   section   discusses   security   and enterprise system management, most specifically HBSS. Individuals with a thorough understanding of this area may consider moving ahead to the Chapter III Conclusion.

D.   SECURITY AND ENTERPRISE SYSTEM MANAGEMENT

This discussion is relevant to the Testing Group as it seeks   to   improve   the   understanding   of   existing   DON procedures for dealing with vulnerabilities, threats, and potential exploits, and how policy compliance verification and remediation are accomplished. This is performed through a discussion of the tools and programs utilized to address these network concerns.

Computer Network Defense Operating System Environment (CND-OSE) is the afloat CND suite that delivers the Host Based Security System (HBSS) and the Secure Configuration Compliance Validation Initiative (SCCVI) upon installation on a platform. The combination of these and their sub-modules form the CND-OSE suite that is now part of the

COMPOSE load. This suite is loaded on every network that has COMPOSE, that is to say, every afloat platform's network [48]. Computer Network Defense Information Assurance Suite (CND-IAS) is the shore-based alternative to CND-OSE and also includes HBSS.

For clarity, the following definitions are provided:

Vulnerability – "existence of a weakness, design, or implementation error that can lead to an unexpected and undesirable event compromising the security of the system." [1]

Threat – "An action or event that might compromise security. A threat is a potential violation of security." [1]

Exploits – "A defined way to breach the security of an IT system through a vulnerability." [1]

1. Intrusion Protection, Intrusion Detection, and Enterprise Network Security Solutions: HBSS

HBSS is the DON enterprise network security solution POR for both afloat and ashore network enterprises. HBSS is being deployed by the DoD to provide security for Windows™ and Unix servers and workstations. A thorough discussion of HBSS is provided in Neff's thesis [7], but HBSS is nonetheless revisited here, as the Testing Group will be testing MAST's ability to interact with HBSS in order to function properly on DON networks.

According to DISA, the primary goal of HBSS is to increase the level of trust with respect to DoD networks and the GIG [49]. HBSS can accomplish this through behavioral, signature, desktop-firewall, and application-

blocking-protections. These remove vulnerabilities and harden DoD networks against threats and exploits. A general description of how HBSS modules perform these four tasks follows [48]:

Behavioral rules are established to identify a profile of network activity. Departure from these rules results in a system alert [48].

The Host Intrusion Prevention System (HIPS) is used to provide signature protection. This works as most standard virus protection software, crosschecking traffic against a database of signature rules to assess whether or not activity is malicious. Malicious activity detection triggers an alert (event) [48].

A firewall is used to filter between the host system and the network or Internet. All network traffic to and from the host is scanned at the packet level and compared against a list of firewall rules [48].

Finally, application blocking prevents the launching of certain executable files on the host system [48].

Pertinent to the MAST testing process is that HBSS and its McAfee Agent and modules, such as the electronic Policy Orchestrator (ePO) Server, HIPS, and Virus Scan Enterprise (VSE), (all discussed in greater detail in Neff's thesis [7]) provide protection from threats and exploits (e.g. buffer overflow, DoS, and Trojan horse) through a variety of defense mechanisms to include detection, signature matching, and interception. A thorough description of the types of threats and exploits that exist are included in

several other MAST theses, principally those written by Taff and Salevski, Neff, and Longoria [6, 7, 9].

However, HBSS and its module complement are not alone sufficient to provide complete defense-in-depth for the vulnerabilities in a network. In fact, no amount of defense is able to maintain network health if good housekeeping procedures are not observed. These include such measures as keeping software versions up to date, loading patches as they become available, proper employment of firewalls, and proper configuration of intrusion detection and prevention systems.

To monitor "good housekeeping", DON utilizes the Secure Configuration Compliance Validation Initiative, the Assured Compliance Assessment Solution, and the Intelligent Agent Security Module. These software tools are discussed in the following section.

2. Policy Compliance Verification

Secure Configuration Compliance Validation Initiative is the current DON policy compliance verification tool for ship and shore systems. In the near future, DON expects to transition to the Assured Compliance Assessment Solution for sea and the Intelligent Agent Security Module for shore networks.

a. *Secure Configuration Compliance Validation Initiative (SCCVI)*

The purpose of SCCVI is to monitor networks for secure configurations to discover vulnerabilities. To do this it checks system compliance with IAVA. Commercially known as eEye Digital Security's Retina Network Security

Scanner, or simply "Retina," SCCVI is used to proactively detect and report network system vulnerabilities and to aid in the remediation of those vulnerabilities within DoD organizations [50, 51].

b. Assured Compliance Assessment Solution (ACAS)

ACAS addresses the need for improvements in current DON vulnerability scanning capabilities. The ACAS Security Center provides the capabilities to allow for management, alerting, and reporting against vulnerability and compliance requirements [52].

According to DISA, ACAS "provides automated network vulnerability scanning and configuration assessment, application vulnerability scanning, device configuration assessment, and network discovery." [52] DISA's PEO-MA provides program management and is supporting the deployment of this capability.

c. Intelligent Agent Security Module (IASM)

The purpose of IASM is to perform "near real-time acquisition and normalization of security event logs and alerts from network and host sensors, firewalls, routers, and OSs; and to perform signature-based analyses of normalized events, allowing anomaly-based assessment of events, which generates alarms [for] unique security attacks." [50]

IASM performs network scanning to determine misuse, fraud, or attack. Data are analyzed and correlated utilizing multi-level IASM servers to create cyber attack profiles in near real-time. The technology "detects novel

58

non-signature attacks with cluster attack analysis and anomalous intrusion detection." [53]

3.   Compliance Remediation

One of the purposes of SCCVI is to help automate the remediation process, ensuring that noncompliant systems return to a secure configuration. This process is called "Compliance Remediation" and is performed via three methods: Information Assurance Vulnerability Alerts, the Online Compliance Reporting System, and the Vulnerability Remediation Asset Manager.

a.   *Information Assurance Vulnerability Alerts (IAVA)*

An Information Assurance Vulnerability Alert is a notification generated when an IA vulnerability is discovered that can result in a threat to DoD networks and systems [54]. IAVAs are distributed to system administrators as they become available, dictating fixes that need to be made to systems based on newly identified vulnerabilities. It is then the system administrator's responsibility to patch systems or make desired configuration changes [55].

The Information Assurance Vulnerability Manager (IAVM) is a program that comes with the COMPOSE load that pushes IAVA software onto each computer. It then manages system compliance with updates and patches required by an IAVA.

Compliance reporting occurs in the Online Compliance Reporting System database [56].

b. *Online Compliance Reporting System (OCRS)*

The OCRS provides a Navy-wide IAVM database that is maintained by NCDOC. It is a program that tracks IAVA compliance of all platforms for the Navy. OCRS also follows IA Vulnerability Bulletins. The purpose of the system is to quickly disseminate vulnerability warnings directly to all network action officers and then to collect and track the vulnerability compliance reports from each Navy command [57].

c. *Vulnerability Remediation Asset Manager (VRAM)*

The Vulnerability Remediation Asset Manager was developed as a complement to SCCVI. The SCCVI User Guide from December 2012 [51] describes VRAM as a "web-based interactive analysis tool and data repository for SCCVI scan data and Centrally Managed Programs/Programs of Record (CMP/POR) baseline vulnerability configuration information." VRAM streamlines vulnerability management by providing a tool to monitor system vulnerabilities and to proactively maintain, validate, and document configurations [51].

VRAM also provides network administrators the ability to assess their systems against a documented baseline. This allows a practical avenue for "identification and remediation of deviations from the approved configuration." [51]

E.   SUMMARY

This chapter examined the quantitative testing environment, current testing and implementation methods, and criteria for cyber programs in the DoD and DON.

Focusing on areas pertinent to the Testing Group, it began with an overview of five DoD range facilities: JCOR, JIOR, DoDIAR, NCR, and NCOR. It next furnished basic information on the shipboard environments, COMPOSE and CANES, followed by the shore environments, NMCI, ONE-Net, and NGEN, to facilitate the Testing Group's understanding and knowledge of them. Finally, it concluded with a discussion of HBSS, SCCVI, and other PORs providing a brief look at DON procedures for dealing with vulnerabilities, threats, and potential exploits, and how policy compliance verification and remediation are accomplished.

MAST must be able to operate in these hardware and software environments in order to meet its objectives as an effective training and evaluation tool for network operators and information security agents. The next chapter describes the test procedures that must be addressed by MAST in order to assure its ability to operate in the environments described above.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. QUANTITATIVE TESTING PROCESS

This chapter opens with definitions of relevant terms and proceeds with the objectives and steps of the quantitative testing process for MAST. The steps in this procedure have been tailored specifically to suit MAST, and they are similar to the steps that would be used to place any piece of hardware or software on the PPL/SSIL (see Definitions). In addition to MAST itself, individual Simware modules and the kill switch's system "roll back" ability will be tested.

A.   DEFINITIONS

1.   PPL/SSIL

For any hardware or software to be used on a Navy network it must have received preapproval by the Navy through a testing process performed by SPAWAR. Items that have acquired this approval are listed in the Preferred Product List/System Subsystem Interface List (PPL/SSIL). These items range from hardware such as a Dell Computer or an iPhone, to software applications such as the Microsoft Office Package.

2.   Simulated-Malware (Simware) Module

This is the portion of MAST Software that specifically simulates malicious activity. Simware modules run on client machines. The Scenario Execution Server sends parameters to a client that then starts the Simware module matching those parameters.

Malware Mimics Architecture

Remote Server
Command and Control server
Sends Scenario information to
the Local Server

Database
Stores Scenario prototypes and
reports generated from
running scenarios

Local Server
The Local Server parses the scenario
sent by the server and translates it
to run on the local network

Once a scenario has run, the Local
Server will report the findings back
to the Remote Server

Clients
Receive specifically
constructed commands
from the Local Server

Return command status
to the Local Server

Figure 9.   Simware Module Execution Processes. From [7].

Simware modules (referred to as "scenarios" in Figure 9) are the piece of MAST that affects the client machines. The effects can be visible to the user, such as throwing up a new window, or invisible, such as port scanning or pinging [14].

3.   Kill Switch

The kill switch instantly stops all active and running processes associated with MAST on the server and client and executes return/reset of the network to its original state prior to running the Software or a Simware module, regardless of whether or not the Simware module scenario has completed. MAST returns to its idle state, but is not uninstalled from the client or server computers [14].

64

4.   Roll Back

Part of the kill switch function that returns/resets the network to its original state after any termination, whether due to kill switch activation or Simware module scenario completion (as determined by local network administrators or predetermined by system architects). MAST returns to its idle state, but is not uninstalled from the client or server computers [14].

B.   OVERARCHING OBJECTIVES OF THE TESTING PROCESS

There are two overall objectives for the quantitative testing process. The first is to ensure that when the MAST Software (hereafter referred to as "the Software") is loaded on a network and in an idle state, it does not interfere with, disable, or otherwise negatively impact that network. Additionally, when the Software is actively running a Simware module on the network, this process will ensure that only specific, previously delineated, and pre-determined negative behaviors are observed.

The second objective is to verify the operation of the kill switch, demonstrating that upon its use, it successfully returns the network to its normal, operational state (that prior to running a Simware module) without interfering with, disabling, or otherwise negatively impacting the network on which it is installed.

The following step-by-step procedure is meant to demonstrate that the Software can function on a network in accordance with the objectives and to ensure interoperability with the network. This is specifically different from demonstrating the functionality of MAST,

which has already been demonstrated. The purpose of this chapter is to define the testing process for MAST as it is loaded on a network in an idle and active state, and to define acceptable parameters (i.e., what is meant by a successful or a passing test) for MAST when it is both in idle mode and executing Simware modules.

The first section of this chapter discusses items that must be considered prior to loading MAST onto a range or testing environment and before any testing can take place. The second section defines the testing process by objective, followed by detailed step-by-step procedures. This includes identifying the item being tested; the process or function the item is expected to run, execute or demonstrate; and the criteria for successful completion of each test. This testing process is patterned after a draft plan proposed by a non-attributable source [58].

C.   PRIOR TO TESTING

Prior to the operational range testing of MAST, a comprehensive list shall be created that identifies all services and processes needed for MAST operation. This list must identify the infrastructure-provided services MAST requires for it to be loaded onto a network and properly operate. It must also include additional program or access requirements that will be necessary for testing.

Specific examples of items and services to be determined and allocated or provided prior to loading, operating, and testing are as follows:
- What hardware is required?
  - Number and types of servers required

- Number of clients required
- What software is required?
    - OS version or versions
    - Applications
    - Anti-Virus functionalities
    - What services and processes are required on the server
    - What services and processes are required on the local client
    - Specific programs or browsers
- What level of connectivity is required, internally and externally, if any?
    - Is the test to be performed on a routed network or a local segment?
- What administrative accesses are required, if any?
- Are there security settings in place that must be changed or that must be put in place in order to test MAST?

Hardware or software that is necessary to accomplish these testing objectives (aside from MAST itself) should be limited to items on the PPL/SSIL. This serves the practical purpose of minimizing the administrative overhead for follow-on tests on operational platform's networks.

Furthermore, in the case of simulation of a shipboard environment to accommodate a shipboard-fielding plan, the version of ISNS that is loaded in the test environment must be considered. This will mitigate unexpected installation, integration, and interoperability risks arising after the testing process has already completed.

The OS or Systems should be identified to ensure compliance with all varieties on different platforms (e.g., Unix, multiple variations of Windows, or other).

Prior to the operational range testing of Simware modules, a comprehensive list shall be created that thoroughly identifies the malicious activity to be simulated by each Simware module (hereafter referred to as "the Parameters"). The Parameters shall define the malicious activities that will be demonstrated and describe how these behaviors will be identifiable in the test network. This will ensure characteristics that are demonstrated are limited to those expected per each Simware module's specific design.

For example, in the case of a Simware module built to exhibit the behaviors and signatures of a worm propagating on the network, the Parameters would describe what effects would be present though not necessarily visible (e.g., port scans), and it would also describe what the visible indicators of this activity are, in this case, an increase in benign traffic traversing the network.
Examples of other possible indicators the Parameters should reference are expected increases in CPU usage for servers or clients, and specific defects or disruptions that are expected.

D. TEST PROCEDURE

Objective 1: Establish the configuration of the network at the range on which testing will occur – The following steps of the testing procedure apply to the installation of MAST on the testing range. They are meant

to ensure PPL/SSIL baseline compliance for equipment and software utilized in the testing process.

Step 1.1: Produce a step-by-step re-configuration for the range that will accommodate the Software.

Criteria for success = comprehensive, easily understood procedure can be safely completed by testers and/or range personnel.

Step 1.1.1: Verify that the step-by-step network re-configuration procedures are architecturally acceptable and follow a logical order. Verify that no steps are skipped; no steps are assumed by default; and that all automatic or requested system reboots are noted.

Step 1.2: Produce step-by-step MAST configuration procedures for range installation.

Criteria for success = comprehensive, easily understood procedure can be safely completed by testers and/or range personnel.

Objective 2: MAST Operational Verification - The original testing requirements call for the completion of SOVT-like checks requested by the PPL/SSIL developer or sponsor. A System Operational Verification Test (SOVT) is an operational test of equipment performed after installation or modification on a Navy platform.

Since the Software is in its initial testing phase, post-installation or –modification testing will not be discussed at this time.

Objective 3: Software Compatibility Checks – The following steps of the testing process apply when the Software is installed on network servers or clients.

Step 3.1: Inspect Application, Security, and System Event Viewers on each affected host before and after installation of the Software.

Criteria for success = no defects.

Step 3.2: Identify and verify critical services and processes on the Primary Domain Controller (PDC) before and after installation of the Software.

Criteria for success = no service disruptions.

Step 3.3: Identify and verify critical services and processes on the alternate (Backup) Domain Controller or Controllers, if applicable, before and after installation of the Software.

Criteria for success = no service disruptions.

Step 3.4: Identify and verify critical services and processes on the Exchange Server before and after installation of the Software.

Criteria for success = no service disruptions.

Step 3.5: Identify and verify critical services and processes on the Management Server before and after installation of the Software.

Criteria for success = no service disruptions.

Step 3.6: Identify and verify critical services and processes on any additional servers before and after installation of the Software.

Criteria for success = no service disruptions.

Step 3.7: Identify and verify critical services and processes on each affected client before and after installation of the Software.

Criteria for success = no service disruptions.

Step 3.8: Identify and verify file, registry setting, or other setting additions and changes made during installation of MAST (to include its Simware modules) and any security vulnerabilities that were potentially introduced. Running an accredited vulnerability scan (i.e., a Secure Configuration Compliance Validation Initiative product such as Retina©) before and after loading MAST will expose vulnerabilities introduced by MAST to the network, if any.

Criteria for success = no new Medium or High vulnerabilities.

Step 3.9: Verify that the Microsoft Suite (Word, Excel, Access, PowerPoint, Outlook and Internet Explorer) Application will function after installation of the Software. Criteria for success = no defects.

Step 3.10: In the event that errors, defects, or disruptions are discovered while accomplishing test steps 3.1 to 3.9, they must be recorded or documented in detail.

Provide a detailed description, and if possible, explanation of errors, defects, or disruptions.

Step 3.10.1: Upon completion of steps 3.1 – 3.7 (and any additional testing identified in steps 3.10.3 and 3.10.4 if applicable), each step will be repeated to analyze the same entity or function before and after running Simware modules.

Criteria for success = defects or service disruptions limited to those predetermined in the Parameters for each individual Simware module.

Step 3.10.2: Following the completion of the actions defined in step 3.10.1, each step will be repeated to analyze the same entity or function before and after activation of the kill switch, as applicable.

Criteria for success = Simware module functionality as described in the Parameters must cease completely. All active or running processes associated with MAST shall end and the network shall return to its state prior to running a Simware module. MAST returns to its idle state, but has not been uninstalled from the network.

Step 3.10.3: Additional to be determined (TBD) inspection and testing on the service or application related to the errors, defects, or disruptions identified in 3.10 may be performed.

Criteria for success = TBD.

Step 3.10.4: Perform any additional inspections or checks that are requested by MAST's developer or sponsor, or required by the test environment.

Criteria for success = TBD.

Objective 4: Host Resource Usage – The following steps of the testing process apply to the interoperation of MAST with the server or client(s).

Step 4.1: Identify the amount of disk space consumed by MAST.

Criteria for success = MAST utilizes less than or equal to 500 Megabytes.

Step 4.2: Inspect the percentage of CPU usage for all clients and the PDC and its alternate; the Exchange Server; Management Servers; and any other existing servers utilized for the testing process with and without the Software loaded.

To test "with and without" here and henceforth indicates first establishing the baseline without the Software loaded, and then checking the difference after loading the Software.

Criteria for success = less than or equal to 5% increase in CPU usage for each client or server.

Step 4.3: Inspect the amount of pages per second on all clients and the PDC and its alternate; the Exchange Server; Management Servers; and any other servers utilized for the testing process with and without the Software loaded.

Criteria for success = less than or equal to 5% increase in amount of pages per second on each client or server.

Step 4.4: Inspect the amount of disk input/output on all clients and the PDC and its alternate; the Exchange Server; Management Servers; and any other servers utilized for the testing process with and without the Software loaded.

Criteria for success = less than or equal to 5% increase in disk input/output on each host.

Step 4.5: Inspect the amount of network adapter use on all clients and the PDC and its alternate; the Exchange Server; Management Servers; and any other servers utilized for the testing process with and without the Software being operated.

Criteria for success = less than or equal to 5% increase in network adapter use on each client/server.

Step 4.6: Inspect the amount of Active Directory database queries on the PDC and its alternate server with and without the Software loaded.

Criteria for success = less than or equal to 5% increase in queries on each effected server.

Step 4.7: Host Intrusion Detection System (HIDS) interaction. Steps 4.7.1 – 4.7.3 of the testing process apply when MAST interoperates with the HIDS.

Step 4.7.1: HIDS and MAST do not conflict during server startup/shutdown.

Criteria for success = no defects.

Step 4.7.2: Check the Site Protector console for new HIDS events. Document all new events for analysis and baseline tuning.

Step 4.7.3: Check the rate at which new events occur. Indicate whether the occurrences are continuous, occur upon start-up, or are periodic.

Step 4.8: In the event of test results that are Out-of-Limits (OOL) or the occurrence of errors, defects, or disruptions while accomplishing test steps 4.1 to 4.7 and all sub-steps, record or document each in sufficient

detail to allow post-test analysis. Provide a detailed description, and if possible, explanation of errors, defects, or disruptions.

Step 4.8.1: Upon completion of steps 4.1 – 4.6 (and any additional testing identified in steps 4.8.3 and 4.8.4 if applicable), each step will be repeated to analyze the same entity or function before and after running Simware modules.

Criteria for success = activity or process being observed for each client or server tested does not exceed level predetermined in the Parameters for each individual Simware module.

Step 4.8.2: Following the completion of the actions defined in step 4.8.1, each step will be repeated to analyze the same entity or function before and after activation of the kill switch, as applicable.

Criteria for success = Simware module functionality as described in the Parameters must cease completely. All active or running processes associated with MAST shall end and the network shall return to its state prior to running a Simware module. MAST returns to its idle state, but has not been uninstalled from the network.

Step 4.8.3: Additional TBD inspection and testing on the service or application related to the OOL results or errors identified in 4.8 may be performed.

Criteria for success = TBD.

Step 4.8.4: Perform any additional inspections or checks that are requested by the Program developer or sponsor, or required by the test environment.

Criteria for success = TBD.

Objective 5: Packet Transport Resource Usage – The following steps apply when the hosting network transports MAST packets.

Step 5.1: Identify the amount of Backbone Layer-3 transport device (switch or router) CPU usage that exists with and without the Software loaded.

Criteria for success = less than or equal to 5% increase in CPU usage on each Backbone Layer-3 transport device.

Step 5.2: Identify spanning tree re-convergence events on the Backbone Layer-2 switch or switches with and without the Software loaded.

Criteria for success = no events.

Step 5.3: Identify Virtual Router Redundancy Protocol re-convergence events on the Backbone Layer-3 transport device (switch or router) with and without the Software loaded.

Criteria for success = no events.

Step 5.4: Identify Open Shortest Path First or other routing protocols utilized on the hosting network, re-convergence events on the Backbone Layer-3 transport device (switch or router) with and without the Software loaded.

Criteria for success = no events.

Step 5.5: Identify memory use on the Backbone device with and without the Software loaded.

76

Criteria for success = less than or equal to 5% increase in memory usage on each Backbone device.

Step 5.6: Identify the amount of inter-network transport device traffic that is generated while the Software is operating normally.

Criteria for success = less than or equal to 5% increase in inter-network transport device traffic.

Step 5.7: In the event of test results that are OOL or the occurrence of errors, defects, or disruptions while accomplishing test steps 5.1 to 5.6, record or document each in sufficient detail to support post-test analysis.

Provide a detailed description, and if possible, explanation of errors, defects, or disruptions.

Step 5.7.1: Upon completion of steps 5.1 – 5.6 (and any additional testing identified in steps 5.7.3 and 5.7.4 if applicable), each step will be repeated to analyze the same entity or function before and after running Simware modules.

Criteria for success = traffic, events, or usage being observed for each client or server tested does not exceed level predetermined in the Parameters for each individual Simware module.

Step 5.7.2: Following the completion of the actions defined in step 5.7.1, each step will be repeated to analyze the same entity or function before and after activation of the kill switch, as applicable.

Criteria for success = Simware module functionality as described in the Parameters must cease

completely. All active or running processes associated with MAST shall end and the network shall return to its state prior to running a Simware module. MAST returns to its idle state, but has not been uninstalled from the network.

Step 5.7.3: Additional TBD inspection and testing on the service or application related to the OOL results or errors identified in 5.7 may be performed.

Criteria for success = TBD.

Step 5.7.4: Perform any additional inspections or checks that are requested by the Program developer or sponsor, or required by the test environment.

Criteria for success = TBD.

Objective 6: WAN (off-ship) Bandwidth Resource Usage – The following steps are applicable if MAST packets are transported to an off-site or simulated off-site location. Such traffic relay would be supported by organic Navy systems, such as ISNS or ADNS. However, such services might be provided by non-organic systems such as commercial satellite or non-government-off-the-shelf radio systems.

Step 6.1: Ship-to-shore and shore-to-ship data communications, where applicable, should be Transmission Control Protocol (TCP) -based. User Datagram Protocol (UDP) -based communications are not permitted with the exception of multicast applications.

Criteria for success = all off-ship data communications are TCP-based, except where explicitly required.

Step 6.2: Where applicable, if ship-to-shore and shore-to-ship Internet protocol IP data communications are

UDP versus TCP-based, how well do they co-exist with other present applications?

Criteria for success = MAST throttles bandwidth demanded to a configurable rate.

Step 6.3: When applicable, ship-to-shore and shore-to-ship IP data communications can be supported by an authorized and mandated proxy server.

Criteria for success = application can be supported by Microsoft© proxy and/or Microsoft© ISA server.

Step 6.4: If applicable, check Network Intrusion Detection System (NIDS) interaction. Steps 6.4.1 – 6.4.3 of the testing process apply when MAST interoperates with the NIDS.

Step 6.4.1: Check Site Protector console for new NIDS events. Document all new events for analysis and baseline tuning.

Step 6.4.2: Determine the rate at which new events occur. Indicate whether the occurrences are continuous, occur upon start-up, or are periodic.

Step 6.4.3: Annotate Ports and Protocols the test system uses for network communications.

Step 6.5: In the event that errors, defects, or disruptions are discovered while accomplishing test steps 6.1 to 6.4 and any sub-steps, record or document each in detail.

Provide a detailed description, and if possible, explanation of errors, defects, or disruptions.

Step 6.5.1: Upon completion of steps 6.1 – 6.4 (and any additional testing identified in steps 6.5.3 and 6.5.4 if applicable), each step will be repeated to analyze the same entity or function before and after running Simware modules.

Criteria for success = traffic, events, or protocol being observed for each client or server tested does not exceed level predetermined in the Parameters for each individual Simware module. In addition, interaction with NIDS (if applicable) must be as was expected in Parameters.

Step 6.5.2: Following the completion of the actions defined in step 6.5.1, each step will be repeated to analyze the same entity or function before and after activation of the kill switch, as applicable.

Criteria for success = Simware module functionality as described in the Parameters must cease completely. All active or running processes associated with MAST shall end and the network shall return to its state prior to running a Simware module. MAST returns to its idle state, but has not been uninstalled from the network.

Step 6.5.3: Additional TBD inspection and testing on the service or application related to the errors, defects, or disruptions identified in 6.5 may be performed.

Criteria for success = TBD.

Step 6.5.4: Perform any additional inspections or checks that are requested by the Program developer or sponsor, or required by the test environment.

Criteria for success = TBD.

Objective 7: Uninstalling MAST – The following steps of the testing procedure are pertinent to the removal of MAST from the testing range.

Step 7.1: Check that instructions follow a logical order, no steps are skipped, no steps are assumed by default, and all automatic or requested system reboots are noted.

Criteria for success = no defects.

Step 7.2: Verify that all MAST folders are deleted during the uninstall process.

Criteria for success = all deleted.

Step 7.3: Verify that any MAST components left on the system(s)are noted as to why they are not deleted.

Criteria for success = all undeleted components are documented.

Step 7.4: Verify that shared .dll and other system files that are not deleted at uninstall are noted. Criteria for success = all undeleted files noted.

E.   SUMMARY

This chapter discussed the step-by-step quantitative testing process for MAST software to satisfy the primary objective of this research and answer the problem statement. In addition, testing processes for the kill switch and Simware modules, two critical functions of MAST, were defined. Chapter V discusses conclusions and our recommendations for the future of MAST, to include development of a Simware module template, implementation, and cost benefit analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND FUTURE WORK

A. CONCLUSIONS

This thesis provides a methodology for the testing phase of the roadmap for fielding MAST to support an installation decision. This phase in MAST's development focuses on the quantitative testing at a DoD cyber range.

The purpose of this thesis is to define a measurable set of procedures that satisfy our objectives stated in Chapter I, to wit, the quantitative testing process for MAST. Meeting this objective requires designing a suite of tests that definitively demonstrate the ability of MAST to perform securely on operational DoD networks.

In addition to MAST's core functionality, the testing process verifies the operations of the kill switch and Simware modules. Verification of the kill switch ensures that it restores the network to its previous configuration, placing MAST in an idle state where it exhibits no negative impact to the network. Simware modules are verified to ensure that when executed they replicate only the nefarious behavior that is expected.

The set of measureable procedures developed for the quantitative testing include accomplishing the following sub-bullets for MAST before, during, and after interaction with an operating network (interoperability):

- Establishing cyber testing range network configurations
- Software compatibility checking
- Verifying host resource usage while MAST is operating

- Verifying packet transport usage resources

- Verifying off-ship/-site bandwidth resource usage

- Establishing methodology for uninstalling MAST from a network

These objectives are satisfied through the procedure laid down in Chapter IV. We have identified a step-by-step procedure, the following of which would perform a thorough and exhaustive, industry-standard testing of MAST and its Simware modules.

Before executing the test procedure, the following will be required:

- Knowledge of DoD range capabilities

- Familiarity with ship and shore network environments

- Understanding of Security and Enterprise System Management

That being the case, the testing environment depicted in Chapter III is valuable for several reasons: it provides a singular location where information regarding this broad area of the cyber domain is collected, because necessary specialization in specific cyber niches and areas of expertise may leave some in the dark when it comes to entire swathes of the cyber testing environment. Furthermore, many are simply unfamiliar with much of the environment because of its staggering breadth relative to its young age.

B. BENEFITS TO THE DON AND DOD

The type of training MAST provides is most similar to what network administrators would experience during a penetration test by a Navy Red Team. Due to the low

availability of Red Teams and the cost associated with them, several NPS students endeavored to create a program that can perform as a Red Team, and meet the needs of the fleet in areas that Red Teams fall short, such as availability and cost [6, 7]. The implementation of MAST as a DON or DoD POR will provide the benefit of training network administrators in the recognition and removal of malware and malicious activities through the use of simulated malware, thus better enabling them to defend DoD networks [7].

This thesis has provided a procedure for testing MAST in order to facilitate its implementation process and provide the administrators of DON and DoD networks with a practical and useful tool to help them successfully defend their networks.

C.   FUTURE WORK

1.   Module Template Development

There are security and practicality concerns involved in the creation of multiple Simware modules utilizing many different sets of coding and scripts. Specifically, it is impractical to return to the test range after the development of each individual Simware module, but this could be necessary for network security reasons.

One solution is the creation of a module template. This could take the form of a program built into a GUI on which the network administrator can input general parameters for the type of malware they would like to simulate. The Testing Group could test such a model concurrently with MAST.

A module template allows for practical creation of Simware modules that meet user's requirements. Additionally, creating Simware modules in the same general way would simplify security testing procedures, thus preventing MAST or the Simware modules from themselves becoming an attack vector.

2. Focus on Fleet Implementation

The need exists to provide MAST, a useful and necessary product, to DoD and DON network administrators in accordance with a timeline sufficiently advanced to meet an already existing threat.

As it is currently constructed, MAST has great potential to provide improved training for DoD network administrators, and is directed at providing a network health management function. This includes utilization of MAST as a method of insuring proper network configuration of other PORs, primarily those concerned with network security, such as HBSS and HIPS. This affords the motivation for maintaining a narrowed focus to ensure concentration on program delivery.

Following successful quantitative testing at a cyber range by the Testing Group, the next steps toward acceptance as a DON POR need to be taken for MAST to be adopted by DoD at large. This means operational testing on a platform at an exercise such as TRIDENT WARRIOR, or on a shore-based network or training environment, and installation on a platform in preparation for a battle group exercise (such as a COMPTUEX).

Individuals in the computer science or cyber fields of study who have experience in POR implementation are likely candidates to perform fleet testing.

3.   Cost Benefit Analysis

There needs to be a supportability and sustainment plan for MAST. There also needs to be a defined fielding strategy that determines if MAST is cost effective through examination of factors such as sustainment and maintenance cost.

A necessary part of implementation is the discovery of costs, e.g., maintenance costs, manpower costs, etc., to determine the benefits to using MAST over current solutions. These can be developed through a business case analysis that evaluates the potential economic benefit of MAST as compared to its closest comparable system and determines the logistical and financial barriers, requirements, and procedures involved in implementation.

Performing a cost benefit analysis will quantify costs vs. savings and identify if MAST provides a net benefit to the DoD. Candidates for this research would be those in a business or logistics field of study with similar backgrounds.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX. CYBER RANGE POINTS OF CONTACT

JIOR - Captain John Moore, USN, is currently Chief, Joint IO Range Branch and Mr. Greg Sisson the Deputy Chief of JIOR gregory.sisson@js.smil.mil.

JCOR - Mr. Tom May manages the JCOR as a whole, but each consortium member manages their own respective Service's simulators. C. D. "SKI" Soltysik Csoltysik@camber.com at (618) 606-1604 is the Lead Cyber Exercise Planner. W. H. Dunn wdunn@camber.com at (850)896-5659 is the VP for Cyber. Mr. Tom May Thomas.may@us.af.mil at (618)229-6277, an Air Force civilian, manages the JCOR as a whole.

DoDIAR - The procedures for connecting to the DoD Information Assurance Range can be obtained by contacting the Cyber Range Customer Management Team at IARangeCMT@itsfac.com. Jeffrey Combs jeffrey.combs@usmc.mil is the Program Manager for USMC C4 and the DoD Cyber IA Range.

NCR – Todd Fisher coordinates NCR test events and can be contacted at todd.g.fisher@osd.mil.

NCOR – LCDR Steven Calhoun Steven.C.Calhoun@navy.mil at (757)417-6720 x9 is the 10TH FLEET, N72 and manages the simulator, and James Powell is Lead Engineer for NCOR and can be contacted via email at James.A.Powell.ctr@navy.mil.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] *Certified Ethical Hacker: Ethical Hacking and Countermeasures*, Courseware Guide v7, Module 1–19, ECCouncil USA, Albuquerque, NM, 2012, pp. *1–57.*

[2] United States Government Accountability Office, *CYBERSECURITY: Continued Attention Needed to Protect Our Nation's Critical Infrastructure.* Washington, D.C., GAO-11-865T, July 26, 2011, pp. *1–16*.

[3] Director of National Intelligence, Statement for the Record on the Worldwide Threat Assessment of the U.S. Intelligence Community, statement before the Senate Select Committee on Intelligence, Feb. 16, 2011.

[4] M. Chertoff, "The Cybersecurity Challenge," *Regulation & Governance,* vol. 2, pp. *480–484,* 2008.

[5] J. Brito and T. Watkins, "Loving the Cyber Bomb," *Harvard Nat. Security J.*, vol. 3, pp. *39–84,* 2011.

[6] W. R. Taff Jr. and P. M. Salevski, "Malware Mimics for Network Security Assessment," M.S. thesis, Dept. Comput. Sci., Naval Postgraduate School, Monterey, California, 2011.

[7] J. M. Neff, "Verification and Validation of the Malicious Activity Simulation Tool (MAST) for Network Administrator Training and Evaluation," M.S. thesis, Dept. Comput. Sci., Naval Postgraduate School, Monterey, California, 2012.

[8] J. Hammond, "Malicious Behavior Expansion," presented at Program Sponsor Brief, Naval Postgraduate School, Monterey, California, 2012.

[9] R. Longoria, "Scalability Assessments for the Malicious Activity Simulation Tool (MAST) for Network Administrator Training and Evaluation," M.S. thesis, Dept. Comput. Sci., Naval Postgraduate School, Monterey, California, 2012.

[10] G. Belli, personal communication of work in progress, M.S. thesis forthcoming, Dept. Comput. Sci., Naval Postgraduate School, Monterey, California, 2013.

[11] E. Lowney, personal communication of work in progress, M.S. thesis forthcoming, Dept. Comput. Sci., Naval Postgraduate School, Monterey, California, 2013.

[12] Department of the Navy, *Navy Tactical Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance Interoperability Procedural Interface Standards Requirements, Certification, and Testing,* OPNAV INSTRUCTION 9410.5C, pp. *1-9*, 2013, Feb. 19.

[13] J. D. Fulp, quote from CS 3690 Network Security, at Naval Postgraduate School, Monterey, California, Aug. 2012.

[14] G. Belli. Question about a definition. [Personal email] (2013, Feb. 13).

[15] J. F. Sandoz, "Red Teaming: A Means for Transformation," Joint Advanced Warfighting Program, Institute for Defense Analysis, Alexandria, VA, Rep. P-3580, January 2001. [Online]. Available: http://www.dtic.mil/cgibin/-GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA388176.

[16] "Automated" in the Free Dictionary. [Online]. Available: http://www.thefreedictionary.com/automated. Accessed Feb 19 2013.

[17] A. Littlejohn and E. Makhlouf, private communication, Aug. 2012.

[18] A. Littlejohn and E. Makhlouf, private communication, Feb. 2013.

[19] "Comprehensive National Cybersecurity Initiative," in *National Security Presidential Directive 54 and Homeland Security Presidential Directive 23.* [Online]. Available: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[20] "2012 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC) Paper No. 12408."

[Online]. Available:
http://ntsa.metapress.com/link.asp?id=8l4tx4h83j68v150

[21] G. T. Sisson. Joint IO Range Brief. [Personal email]
(2012, Dec. 3).

[22] J. A. Combs. DoD Cyber Range. [Personal email] (2012,
Nov. 5).

[23] W. Dunn. Request for information. [Personal email]
(2012, Nov. 28).

[24] "DoD IA Range Documents." *IA Range Brief* [Online].
Available: https://c4.hqi.usmc.mil/.

[25] "DoD IA Range Home." [Online]. Available:
https://c4.hqi.usmc.mil/.

[26] Lockheed Martin (2012, Dec. 3). *NCR Program Overview*
[PowerPoint]. Accessed 14 Nov 12.

[27] J. A. Powell. Navy Cyberspace Operations Range (NCOR)
Overview. [Personal email] (2012, Oct. 17).

[28] "USN begins CANES installations aboard destroyer
fleet," in Defense & Security Intelligence & Analysis:
IHS Jane's. [Online]. Available:
http://www.janes.com/products/janes/defence-security-
report.aspx?id=1065974757.

[29] "The Common PC Operating System Environment Program –
COMPOSE." [Online]. Available:
http://www.doncio.navy.mil/chips/ArticleDetails.aspx?I
D=3044.

[30] "Naval Enterprise Networks." [Online]. Available:
http://www.doncio.navy.mil/TagResults.aspx?ID=113.

[31] "Space and Naval Warfare Systems Command (SPAWAR)."
[Online]. Available:
http://www.public.navy.mil/spawar/Pages/default.aspx.

[32] "PEO C4I > About Us." [Online]. Available:
http://www.public.navy.mil/spawar/PEOC4I/Pages/AboutUs
.aspx.

[33] "Engineering Services: Software Support," in SSES NexGen. [Online]. Available: http://www.sses-nexgen.com/es-ss_compose.html.

[34] SPAWAR System Center Charleston (2006, September 20). Software version description for COMPOSE (version 3.0.0.1 revision 12), pp. *1*.

[35] "U.S. Navy 2012 Program." [Online]. Available: http://www.navy.mil/navydata/policy/seapower/npg12/top -npg12.pdf

[36] "Consolidated Afloat Networks and Enterprise Services (CANES)." [Online]. Available: http://www.public.navy.mil/spawar/productsServices/Pag es/ConsolidatedAfloatNetworksandEnterpriseServicesCANE S.aspx.

[37] Harry. J. Thie, Margaret C. Harrell, Aine Seitz McCarthy and Joseph Jenkins. Consolidated Afloat Networks and Enterprise Services (CANES): Manpower, Personnel, and Training Implications. Santa Monica, CA: RAND Corporation, 2009. [Online]. Available: http://www.rand.org/pubs/monographs/MG896. Also available in print form. p.26

[38] "Consolidated Afloat Networks and Enterprise Services (CANES)." Integrated Evaluation Framework (IEF), Commander, Operational Test and Evaluation Force's (COMOPTEVFOR) 3980 (1743-OT-B1), Ser 647/SXXX, May 11, 2012, pp. *1-3*.

[39] "PEO EIS > Naval Enterprise Networks (NEN)." [Online]. Available: http://www.public.navy.mil/spawar/PEOEIS/NEN/Pages/def ault.aspx.

[40] "Navy Marine Corps Intranet - Program Milestones." [Online]. Available: http://www.public.navy.mil/spawar/PEOEIS/NEN/NMCI/Docu ments/NMCI%20Program%20Milestones.pdf

[41] "Navy Marine Corps Intranet (NMCI) > About NMCI" [Online]. Available: http://www.public.navy.mil/spawar/PEOEIS/NEN/NMCI/Page s/AboutUs.aspx.

[42] "NMCI Continues to Offer Solutions for Diverse Mission Needs." [Online]. Available: http://www.doncio.navy.mil/ContentView.aspx?ID=3928.

[43] "What is NGEN?" [Online]. Available: http://www.doncio.navy.mil/ContentView.aspx?ID=588.

[44] "What NMCI Means to Us." [Online]. Available: http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=3696.

[45] "ONE-Net." [Online]. Available: http://www.public.navy.mil/fcc-c10f/nctsfe/Pages/ONE%20NET.aspx.

[46] "Naval Enterprise Networks (NEN) > OCONUS Navy Enterprise Network (ONE-Net)." [Online]. Available: http://www.public.navy.mil/spawar/PEOEIS/NEN/ONE-Net/Pages/default.aspx.

[47] "What's Next for NGEN?" [Online]. Available: http://www.doncio.navy.mil/ContentView.aspx?ID=4159.

[48] ManTech, *CND-OSE Training Guide* (version 1.2), July 17, 2011, pp. *1-27*.

[49] Defense Information Systems Agency, *Host Based Security System (HBSS) Technology Overview* (Version 4, Release 3), Jan. 2013, pp. *1-7*.

[50] Chief Information Officer, Department of the Navy, *Computer Network Defense Roadmap* (version 1.1), May, 2009, pp. *1-19*.

[51] SPAWAR, *Secure Configuration Compliance Validation Initiative (SCCVI) User Guide* (version 2.1), Dec. 2012, pp. *1-44*.

[52] "Assured Compliance Assessment Solution." [Online]. Available: http://www.disa.mil/Services/Information-Assurance/SCM/ACAS.

[53] "Intelligent Agent Security Module (IASM)." [Online]. Available:

http://www.dodtechmatch.com/DOD/SuccessStories/View.as px?id=60117.

[54] Committee on National Security Systems, *National Information Assurance (IA) Glossary* (CNSSI No. 4009), Apr. 2010, pp. *36.*

[55] "Patch the GIG." [Online]. Available: http://www.disa.mil/Services/Information-Assurance/SCM/Patch-the-GIG.

[56] "Online Compliance Reporting System database." [Online]. Available: https://www.iava.navy.mil.

[57] D. Crotty (2008, May 21), *Defense Systems Focus on IA Seminar.* [Online]. Available: http://events.fcw.com/events/2008/DS1/downloads/DS_San %20Diego_Crotty.pdf

[58] J. H. Gibson, private communication, 26 March 2013.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
    Ft. Belvoir, Virginia

2. Dudley Knox Library
    Naval Postgraduate School
    Monterey, California

3. Captain David Aland, USN, (Ret.)
    Office of the Director, Operational Test & Evaluation
    Washington, D.C.

4. Dr. Gurminder Singh
    Naval Postgraduate School
    Monterey, California

5. Mr. John H. Gibson
    Naval Postgraduate School
    Monterey, California

6. Commander Joe Sullivan, USN
    Naval Postgraduate School
    Monterey, California

7. Dr. Duane Davis
    Naval Postgraduate School
    Monterey, California

8. Dr. Cynthia Irvine
    Naval Postgraduate School
    Monterey, California