2010-09

Bridging the gap in the realm of information dominance a concept of operations for the Naval Postgraduate School Center for Cyber Warfare

Duke, Cynthia R.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

BRIDGING THE GAP IN THE REALM OF INFORMATION DOMINANCE: A CONCEPT OF OPERATIONS FOR THE NAVAL POSTGRADUATE SCHOOL CENTER FOR CYBER WARFARE

by

Cynthia R. Duke

September 2010

Thesis Co-Advisors:	Tri Ha
	Vicente Garcia
Second Reader:	John Van Hise

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Bridging the Gap in the Realm of Information Dominance: A Concept of Operations for the Naval Postgraduate School Center for Cyber Warfare		**5. FUNDING NUMBERS**	
6. AUTHOR(S) Cynthia R. Duke			
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**	

13. ABSTRACT (maximum 200 words)

As the information age continues to evolve and technological expansion persists in creating a marked footprint across the four corners of the world, the need arises to protect our prized assets from potential adversarial motives. The extant threat to cyberspace necessitates the need to aptly man, train, and equip our forces to ably combat any untoward incidents. The Naval Postgraduate School with its very diverse population presents an exact medium to develop this next generation of warriors skilled in the field of Cyber Warfare to project both offensively and defensively against any contingent threat. As its mission statement professes:

> NPS strives to provide relevant and unique advanced education and research to increase the combat effectiveness and enhance the security of the United States.

This thesis will leverage current instructions to bridge the gap and focus on providing a Concept of Operations for the Center for Cyber Warfare that aligns with the Chief of Naval Operations' (CNO) Strategic Focus Areas. This thesis will additionally recommend an architectural framework that addresses the current issues within the cyber domain and/or will allow for future expansion of the NPS mission datasets deemed of importance to the U.S. Military service and its allies.

14. SUBJECT TERMS Cyber Warfare, Information Dominance			**15. NUMBER OF PAGES** 102
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

BRIDGING THE GAP IN THE REALM OF INFORMATION DOMINANCE: A CONCEPT OF OPERATIONS FOR THE NAVAL POSTGRADUATE SCHOOL CENTER FOR CYBER WARFARE

Cynthia R. Duke
Lieutenant, United States Navy
B.S., University of Santo Tomas, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2010

Author: Cynthia R. Duke

Approved by: Tri Ha
Thesis Co-Advisor

Vicente Garcia
Thesis Co-Advisor

John Van Hise
Second Reader

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

As the information age continues to evolve and technological expansion persists in creating a marked footprint across the four corners of the world, the need arises to protect our prized assets from potential adversarial motives. The extant threat to cyberspace necessitates the need to aptly man, train, and equip our forces to ably combat any untoward incidents. The Naval Postgraduate School with its very diverse population presents an exact medium to develop this next generation of warriors skilled in the field of Cyber Warfare to project both offensively and defensively against any contingent threat. As its mission statement professes:

> NPS strives to provide relevant and unique advanced education and research to increase the combat effectiveness and enhance the security of the United States.

This thesis will leverage current instructions to bridge the gap and focus on providing a Concept of Operations for the Center for Cyber Warfare that aligns with the Chief of Naval Operations' (CNO) Strategic Focus Areas. This thesis will additionally recommend an architectural framework that addresses the current issues within the cyber domain and/or will allow for future expansion of the NPS mission datasets deemed of importance to the U.S. military service and its allies.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ABET	Association Board of Engineering and Technology
AC	Alternating Current
ADF	Aerospace Data Facility
ADM	Admiral
AFISRA	Air Force Intelligence, Surveillance, and Reconnaissance Agency
AFIT	Air Force Institute of Technology
AG	Aviation Aerographers Mate
ARFORCYBER	Army Forces Cyber Command
ARPANET	Advanced Research Projects Agency Network
ATM	Asynchronous Transfer Mode
BBN	Bolt, Beranek, and Newman
BF	Beam Forming
BMD	Ballistic Missile Defense
BOF	BackOfficer Friendly
BPS	Bytes Per Second
BSEE	Bachelor of Science in Electrical Engineering
C2	Command and Control
C4	Command, Control, Communications, and Computers
C10F	Commander, United States Tenth Fleet
CAPT	Captain
CCOP	Cryptologic Carry On Program
CCW	Center for Cyber Warfare
CDMA	Code Division Multiple Access
CDROM	Compact Disc Read Only Memory
CED3	Center for Educational Design, Development, and Distribution
CGI	Coast Guard Intelligence
CHDS	Center for Homeland Security and Defense
CI	Cebrowski Institute

CIA	Central Intelligence Agency
CJSEW	Center for Joint Services Electronic Warfare
CNA	Computer Network Attack
CNCI	Comprehensive National Cybersecurity Initiative
CND	Computer Network Defense
CNDRA	Computer Network Defense Response Action
CNE	Computer Network Exploitation
CNO	Chief of Naval Operations
CNO	Computer Network Operation
COCOM	Combatant Commander
COI	Community of Interest
CONOP	Concept of Operation
COTS	Commercial Off the Shelf
CRADA	Cooperative Research and Development Agreement
CS	Computer Science
CT	Cryptographic Technician
CYBERFOR	Cyber Forces Command
DA	Defense Analysis
DC	Direct Current
DDoS	Distributed Denial of Service
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DHS-NCSD	Department of Homeland Security National Cyber Security Division
DIA	Defense Intelligence Agency
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DNI	Director of National Intelligence
DoD	Department of Defense
DONCIO	Department of the Navy Chief Information Officer
DOT	Department of Treasury
DSL	Digital Subscriber Line

DTK	Deception Toolkit
EBK	Essential Body of Knowledge
EC	Electrical and Computers
ECC	Error Correcting Code
ECE	Electrical and Computer Engineering
ECM	Electronic Countermeasure
EE	Electrical Engineering
EPA	Educational Partnership Agreement
ESX	Elastic Sky X
EW	Electronic Warfare
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FLTCYBERCOM	Fleet Cyber Command
FP6	Sixth Framework Program
FuTURE	Future Technology for Universal Radio Environment Project
GB	Gigabyte
GEN/Gen	General
GEOINT	Geospatial Intelligence
GUI	Graphical User Interface
HSPD	Homeland Security Presidential Directive
HUMINT	Human Intelligence
HVAC	Heating, Ventilating, and Air Conditioning
I&A	Intelligence and Analysis
IA	Information Assurance
IC	Intelligence Community
IDC	Information Dominance Corps
IDS	Intrusion Detection System

IEEE	Institute of Electrical and Electronics Engineers
IMINT	Imagery Intelligence
IMT	International Mobile Telecommunications
INR	Bureau of Intelligence and Research
IO	Information Operation
IP	Internet Protocol
IPv4	Internet Protocol version 4
IS	Intelligence Specialist
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technician
ITACS	Information Technology and Communications Services
ITU	International Telecommunications Union
IW	Information Warfare
JIOWC	Joint Information Operations Warfare Center
JP	Joint Publication
JTF	Joint Task Force
KB	Kilobit/byte
LAN	Local Area Network
LIDAR	Light Detection and Ranging
LOO	Lines of Operation
LTE	Long Term Evolution
MARFORCYBER	Marine Corps Forces Cyber Command
MASINT	Measurement and Signals Intelligence
MCIA	Marine Corps Intelligence Activity
MDA	Maritime Domain Awareness
MEng	Master of Engineering
MI	Army Military Intelligence
MIMO	Multiple-Input Multiple-Output

MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MS	Master of Science
MSCE	Master of Science in Computer Engineering
MSDNAA	Microsoft Developer Network Academic Alliance
MSEE	Master of Science in Electrical Engineering
MSES(CE)	Master of Science in Engineering Science with a major in Computer Engineering Electrical Engineer
MSES(EE)	Master of Science in Engineering Science with a major in Electrical Engineering
MULTI-INT	Multiple Source Intelligence
NAP	National Academy Press
NAS	National Academy of Sciences
NAVAIR	Naval Air Systems Command
NAVNETWARCOM	Naval Network Warfare Command
NAVSEA	Naval Sea Systems Command
NETOPS	Network Operations
NGA	National Geospatial-Intelligence Agency
NGMC	Next Generation Mobile Communication
NIC	Network Interface Card
NMS	National Military Strategy
NPS	Naval Postgraduate School
NRO	National Reconnaissance Office
NSA/CSS	National Security Agency/Central Security Service
NSF	National Science Foundation
NSPD	National Security Presidential Directive
NSS	National Security Strategy
NT	New Technology
NTIA	National Telecommunications and Information Administration
NTOC	NSA/CSS Threat Operations Center
NTT	Non-Tenure Track

NWDC	Naval Warfare Development Command
OICI	Office of Intelligence and Counterintelligence
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal Frequency Division Multiple Access
ONI	Office of Naval Intelligence
OPE	Operational Preparation of the Environment
OPNAV	Office of the Chief of Naval Operations
OSRD	Office of Scientific Research and Development
PDDNI	Principal Deputy Director of National Intelligence
PhD	Doctor of Philosophy
PI	Principal Investigator
POTS	Plain Old Telephone Service
POTUS	President of the United States
PQS	Personnel Qualification Standards
QoS	Quality of Service
RAID	Redundant Array of Independent (or Inexpensive) Disks
RAM	Random Access Memory
RDIMM	Registered Dual In-Line Memory Module
RDML	Rear Admiral Lower Half
RF	Radio Frequency
RFC	Request For Comment
ROE	Rules of Engagement
RTRG	Real Time Regional Gateway
SAR	Synthetic Aperture Radar
SATA	Serial Advanced Technology Attachment
SCIF	Sensitive Compartmented Information Facility
SCSI	Small Computer System Interface

SDLC	System Development Life Cycle
SECDEF	Secretary of Defense
SECNAV	Secretary of the Navy
SIGINT	Signals Intelligence
SME	Subject Matter Expert
SNAC	Systems and Network Attack Center
SOA	Service Oriented Architecture
SOP	Standard Operating Procedure
SPAWAR	Space and Naval Warfare Systems Command
STEM	Science, Technology, Engineering, Mathematics
TAO	Tailored Access Operations
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	Time Division Multiple Access
TOE	TCP/IP Offload Engine
TT	Tenure Track
TYCOM	Type Commander
UDIMM	Unregistered Dual In-Line Memory Module
UPS	Uninterruptible Power Supply
USC	University of Southern California
USCYBERCOM	United States Cyber Command
USG	United States Government
USNA	United States Naval Academy
USSTRATCOM	United States Strategic Command
VADM	Vice Admiral
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
VTE	Video Tele Education

WiMAX	Worldwide Interoperability for Microwave Access
WSJ	Wall Street Journal
WWI	Worldwide Wireless Initiative
WWRF	Wireless World Research Forum

EXECUTIVE SUMMARY

This Concept of Operations (CONOP) document provides a functional overview of the Center for Cyber Warfare (CCW). The CCW is envisioned as a joint research venture between the Naval Postgraduate School (NPS) and various military, national, and industry sponsors including—United States Cyber Command (USCYBERCOM); United States Fleet Cyber Command (FLTCYBERCOM)/10th Fleet; the National Security Agency/Central Security Service (NSA/CSS); Department of Homeland Security (DHS); National Geospatial-Intelligence Agency (NGA); Defense Intelligence Agency (DIA); Central Intelligence Agency (CIA); and the National Reconnaissance Office (NRO) to name a few. Additionally, through planned academic partnerships with the University of Southern California (USC) and nine other accredited universities, NPS will participate in an outreach program to educate and train future cadres of cyber warfare professionals. The CCW is NPS's premier site for education, research, and the development of full spectrum cyberspace operational capabilities across all domains. The CCW intent is to operate in direct support of the NPS stated mission by providing the tools to facilitate higher learning of civilians and military officers, and produce the knowledge, technology, and techniques needed by the U.S. and its allied forces to further enhance national security and global initiatives.

The CCW will accomplish this by performing three major functions:

- Producing military officers and civilians that are technically educated and gain expertise in the cyber warfare related disciplines of networks, cryptology/signals intelligence (SIGINT), information operations (IO), cyber, electronic warfare (EW), and space via in residence work and/or distance learning.
- Conducting advanced technical research at the undergraduate and postgraduate levels utilizing the Student Outreach and/or Science, Technology, Engineering, and Mathematics (STEM) Program in addition to NPS associate faculty and Staff guidance.
- Producing guided written theses and technical reports and furthering advancement of cyber techniques applicable for operational use enhancing radio frequency (RF) spectrum dominance (Knorr, 2010).

This CONOP further details the mission of the CCW and the competency areas it will maintain, defines the supporting and supported relationships, and describes the material and personnel requirements needed to accomplish the mission. An appendix to the CONOP includes a proposed architectural framework for the Honeynet laboratory.

ACKNOWLEDGMENTS

First and foremost, I would like to thank my thesis advisors, Professor Tri Ha and CAPT Vicente Garcia, for bringing me under their wings and providing direction both academically and professionally, throughout my stay here at Naval Postgraduate School. To CDR John Van Hise, your notable work ethic and assistance in providing academic fluidity and a diverse perspective on the organization of my thesis is very much appreciated. To the ECE Department faculty and staff, particularly Dr. Jeffrey Knorr, for providing me the opportunity to immerse myself and be a part of team that helped build the foundation for the Center for Cyber Warfare, thank you very much. Thanks to all my professors, who in one way or another have imparted some explicit knowledge upon which I can apply in my future professional career path.

I would be remiss if I did not thank those in my personal life who helped along the way, especially my mom and dad, family, fellow students, and countless friends I have made along the way. To my husband, Quinn, and our son, Landon. Their love and understanding provided me strength to see through the rough patches that come with attaining one's Master's. Thank you both from the bottom of my heart.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

I'M THE CREEPER–CATCH ME IF YOU CAN…

Imagine, this very phrase replicating itself as it infected multiple host computers. Derived from what would eventually be known as the first "computer virus," labeled the "Creeper" code, it was created by engineers from Bolt, Beranek, and Newman (BBN) Technologies, and deployed not as a malicious code, but rather as an experimental self-replicating program that intrinsically could be brought back to its normal state by a corresponding program named Reaper. While the importance of being able to replicate and repair was the focal point of the experiment, insight and research into the likely consequences and/or future advent of a new era—particularly that of analogous intrusive software programs that could be introduced into a network by an adversary and possibly pose a great threat to society and national security may well have been a worthwhile initiative to follow. And while these concerns for security might not have been readily apparent at the time, most likely due to fact that in 1970 the systems all existed on the closed network architecture Advanced Research Projects Agency Network (ARPANET), the predecessor to what we know today as the Internet, our reliance on such technology presents the case that it is an issue worthy for consideration.

Case in point, data obtained from open source documentation shows a dramatic upward trend from 360,985,492 to 1,966,514,816 of total Internet users worldwide that equates to approximately a 444.8% increase in users since December 2000 (Internet World Stats, 2010)!

The exponential rate at which these numbers continue to propagate, coupled with the progressive ephemeralization of technology, has led us down the path where we now find ourselves facing challenges such as the rapid depletion of available Internet Protocol version 4 (IPv4) addresses, bandwidth allocation, the transition to the next generation data networks, and pervasive threats such as Internet security and database breaches, to include malicious software (malware) attacks and similar vulnerabilities.

The significance of the problem is so pronounced that following the 9-11 attack and more importantly Wall Street Journal's (WSJ) disclosure that terrorists had infiltrated the U.S. power grid and planted malicious code to disrupt the grid, then President George W. Bush ordered the development of National Security Presidential Directive (NSPD) 16 Guidelines for Offensive Cyber-Warfare (Bush, 2002). Open source reporting indicates the directive provides National-level guidance and addresses when and how the United States would launch cyber-attacks against enemy computer networks (Carvalho & da Silva, 2009, p. 12). Promulgation of directives such as NSPD 54 and Homeland Security Presidential Directive (HSPD) 23 on "Cyber Security and Monitoring" further identified the preventative measures being undertaken to secure the cyber environment (Bush, 2008).

Additionally, President Barak Obama more recently called for a complete review of the National Strategy to Secure Cyberspace and the Comprehensive National Cybersecurity Initiative (CNCI). The final CNCI assessment specified the following key lines of reasoning:

- Establishment of a front line of defense from imminent threats through creation or enhancement of shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and ultimately with state, local, and tribal governments and private sector partners.
- Defense from full spectrum threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.
- Strengthen cyber security domain by sustaining cyber education. (Obama, 2010)

The wheels have already been set in motion to operationally accomplish these objectives from the Secretary of Defense (SECDEF) to the CNO through administrative action and establishment of commands that will forge ahead in achieving the required cyberspace effects at the strategic, operational, and tactical levels of war.

At the time of this writing, per SECDEF direction United States Strategic Command (USSTRATCOM) headed by General (Gen) Kevin Chilton established United States Cyber Command (USCYBERCOM) with GEN Keith Alexander assuming the role

of sub-unified commander. This in turn spearheaded the formation of specific service components, namely—Army Forces Cyber Command (ARFORCYBER) supported by NETCOM/9th Signal Command, 1st Information Operations Command, and Intelligence and Security Command; 24th United States Air Force supported by the 688th Information Operations Wing (IOW) and 67th Network Warfare Wing (NWW), United States Fleet Cyber Command (FLTCYBERCOM); and Marine Corps Forces Cyber Command (MARFORCYBER) each of which have been duly charged to sustain cyber operation and defense of networks across the multidimensional battlespace.

To drive home the point, Chief of Naval Operations (CNO) ADM Roughead further elucidated:

> The opening rounds of the next war will be in cyberspace—the Navy must be ready to prevent wars as well as win them; to that, we must understand how we will live, operate and win in cyberspace.

To endorse this, during Fiscal Year (FY) 2010 several key initiatives evolved. Late 2009 witnessed the consolidation of the Chief of Naval Operations (OPNAV) N2/N6 staff and its shift of focus from a platform centric approach to integration of information intensive programs and capabilities, namely—intelligence, surveillance, and reconnaissance (ISR); electronic warfare (EW); information warfare (IW); cyber; maritime domain awareness (MDA); networks; Command, Control, Communications, and Computers (C4); space; unmanned resources; and oceanography all under one umbrella. In January 2010, United States Fleet Cyber Command / Tenth Fleet (FLTCYBERCOM/10th Flt) was established as the U.S. Navy's component command responsible for cyber operations. Finally, to strengthen the number of cyber professionals and the Navy's ability to provide decision superiority to the warfighter the Information Dominance Corps (IDC) was established. Focusing on unity of effort and the capacity to direct a cadre of officers, enlisted, and their civilian counterparts, the IDC integrates Information Professional (IP), Information Warfare (IW), Naval Intelligence, and Oceanography, Space Cadre officers, Cyber Warfare Engineers; and Aviation Aerographers Mate (AG), Cryptologic Technician (CT), Intelligence Specialist (IS), and

Information Technician (IT) enlisted personnel; and civilians with the Navy Defense Civilian Intelligence Program to efficiently deliver information and decision superiority across the cyber environment.

To more clearly understand the concept of information dominance in the cyber domain, one must ask what exactly is cyberspace and how might war be waged in such an environment? Joint Publication (JP) 1-02 defines cyberspace as:

> A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

A more concise description would be that defined by Webster as:

> The online world of computer networks and especially the Internet. (Cyberspace, 2010)

The Information Age has brought us to the point wherein globally people have shifted reliance on computing technology and the Internet as the foundation for enabling its economic, political, social, business, and military sectors. While the cyber infrastructure might perceptibly be more observable and evolutionary in terms of increased productivity, efficiency, and modernization; dependence on these systems presents links to potential security vulnerabilities risks as well as offers undue resilience to cyber attacks backed by state and non-state actors.

Cyber attacks in this case references:

> Deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks. (Owens, Dam, & Lin, 2009)

Figure 1 provides a graphical representation of the evolution of a standard cyber attack process. Five sequential escalatory processes define the initiation of a cyber attack.

- Phase I reconnaissance involves covert collection of information on an unknowing subject either through Web based methods or social engineering tactics.

- Phase II scanning performs a broad range of network mapping that assists in identifying security flaws or vulnerabilities in networks thus allowing the adversary access to and potential compromise of systems.
- Phase III or unauthorized access to systems utilizing password guessing techniques and vulnerability exploitation tools stems from software and hardware design flaws, improper security administration and application of incorrect network management procedures.
- Phase IV or malicious activity refers to those actions that constitute a threat to network or computer systems and includes actions such as data deletion, theft, alteration, and storing of malware on an unsuspecting user's computer.
- All previous phases culminate with Phase V, the exploitation of such data and ability of these attackers to use this information to their advantage in an illegitimate manner.

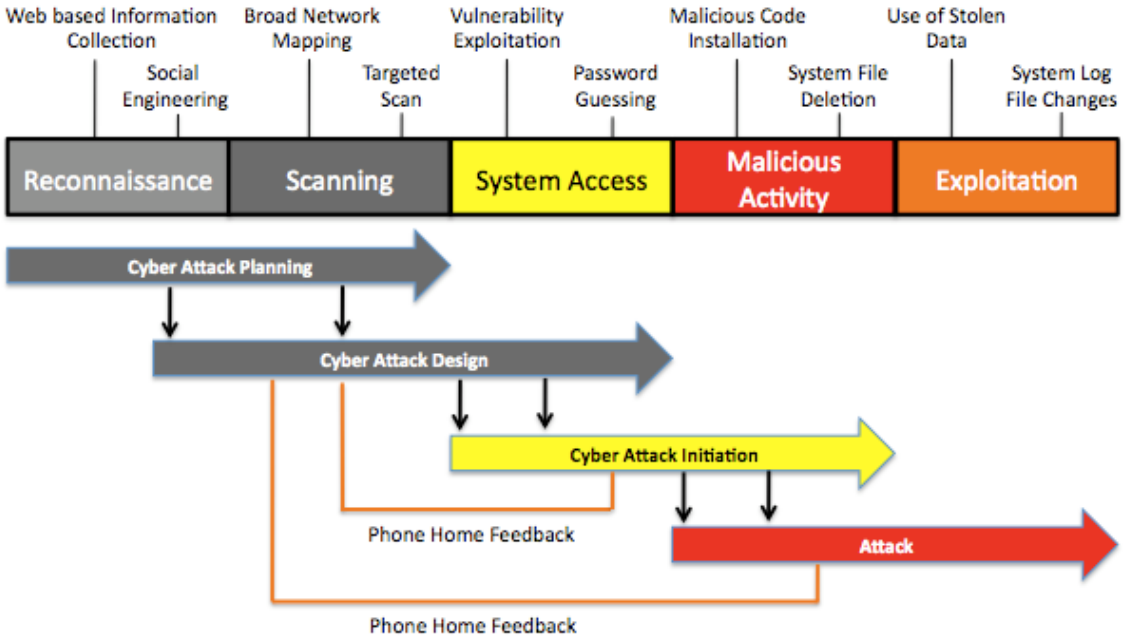

Figure 1. Standard Cyber Attack Process (From Technolytics, 2009)

Instances of historical attacks that utilized similar attack patterns in the cyber domain and have geographical-strategic implications include the following:

- Israeli penetration of Syrian Command and Control (C2) systems.

Under a cloak of darkness, Israeli fighters targeted a Syrian construction site that was believed to contain or process nuclear material. What was interesting in this incident was Israel's ability to penetrate the active Syrian air defense systems unnoticed. This has led to speculations that Israel currently possesses advanced technology to disrupt an adversary's Command and Control (C2) at will. Analysis of this particular attack attributes that through the application of light and electromagnetic pulses Israel transmitted 1s and 0s that effectively masked their tracks on Syrian defense systems (Clarke & Knake, 2010, p. 1–8).

- Russian attack on Estonia's infrastructure.

In the case of Estonia, longstanding tensions between the locals and ethnic Russians and the Bronze Night incident escalated to a suspected Russian attack on their network infrastructure. What is interesting to note is that Estonia ranks high on the list of the most interconnected or wired nations in the world. Utilizing a distributed denial of service (DDoS) attack, servers were flooded with Internet traffic that crashed and shut down multiple Internet services such as e-commerce, government, and broadcasting sites (Clarke & Knake, 2010, p.12–13).

- The synchronized campaign against the country of Georgia.

In 2008, Georgia experienced similar DDoS attacks on their government sites during the Georgia-Russia conflict. The fact that their nodes and routers ran through Russia and Turkey effectively shut Georgia off from the outside world but more importantly it crippled Georgia's banking and financial sector (Clarke & Knake, 2010, p.17–21).

- The "Ghostnet Project" that uncovered a large-scale cyber spying operation with nodes tracing back to the People's Republic of China.

Ghostnet, which spanned 103 countries and infected approximately 2,000 workstations, was of particular significance due to the fact that the targeted computers resided in foreign embassies. Ghostnet had the ability to initiate data and file-capture and remote activation of audio-visual devices so the attacker could eavesdrop on discussions particularly those related to Tibetan issues (Delbert & Rohozinski, 2009).

- The recent cyber attack against Google coined "Operation Aurora."

From December 2009 to January 2010, China was accused of executing malicious attacks against Google and 20 high profile organizations. The incident received worldwide attention and led to Google's review of business relations with China and subsequent request for attack analysis by cyber experts from the National Security Agency (NSA) (Higgins, 2010).

From the preceding examples one can infer that the volatile nature of the cyber environment and the potential expansion of cyber attacks calls for a more proactive role in ensuring the U.S. remain at the forefront in research and development, education, and training of a cyber cadre. In adopting the above directives and in support of operational requirements identified by the recently incepted Cyber Commands, the CCW thus intends to recruit, groom, educate, and invest in a technically adept and cleared cyber workforce to revolutionize the objective of Information Dominance.

A. BACKGROUND

The area of research for this thesis includes a review of past, current, and preliminary and/or draft documents pertaining to cyberspace policy. This thesis builds on these strategies and in accordance with the Naval Postgraduate School's mission and functional requirements, applies these concepts by way of a proposed CONOP for the CCW. Additionally, this thesis addresses requisite CCW cyber infrastructure requirements to generate a more robust experimentation and testing environment.

B. OBJECTIVES

In more specific terms, the objectives of this thesis were to:

- Define the current cyberspace environment to include the key stakeholders from both government and private sectors.
- Develop the foundation for the establishment of a center focused on key cyber warfare mission sets while capitalizing on supporting and piloting emerging technologies.

C. STATEMENT OF PROBLEM

Reliance on information technology initially, as a medium for exchange of unclassified scientific research, has evolved to a more complex network architecture that connects millions of computers on a global scale, supporting numerous business services and functionalities. To respond, to reduce our vulnerability, and to minimize damage and downtime associated with potential adversary and malicious cyber attacks, we need a more comprehensive strategy that addresses cyber security and cultivates training and education for the next generation cyber force.

Key research questions addressed include:

- What is cyber warfare?
- Who are the key stakeholders in this discipline?
- What is the proposed CONOP for the Center for Cyber Warfare?
- How do we develop an architectural framework that can capture changes and future expansion of the center?

D. SCOPE, LIMITATIONS, AND ASSUMPTIONS

The scope of this thesis was limited to analyzing and developing a CONOP for the Cyber Warfare Center because:

- Specific mission capabilities and requirements for the CCW have not been fully defined.
- Research Principal Investigators (PI) need to ensure CCW establishes a service oriented architecture (SOA) framework to fully support collaboration and engagement with other universities, research centers, laboratories, and applicable agencies.
- Recommendations for an extensible and flexible architecture guarantees more efficient and cost effective use of resources.

E. METHODOLOGY AND ORGANIZATION

The research method incorporated a review of existing policy documents and material pertaining to cyber warfare and information dominance. It additionally involved

assisting the CCW Tiger Team in gathering requirements particularly the scope of work for the facility and the server room and the equipment list for the CCW laboratory and administrative spaces as well as the server room.

The succeeding chapters will discuss the CONOP, provide an architectural framework, and submit recommendations and conclusions for the CCW.

THIS PAGE INTENTIONALLY LEFT BLANK

II. PROPOSED CONCEPT OF OPERATIONS—CENTER FOR CYBER WARFARE

A. MISSION AND VISION

In consonance with explicitly stated national, strategic, and operational guidance, and under the auspices of the Naval Postgraduate School, the Center for Cyber Warfare (CCW) provides a full spectrum graduate-level facility that enables seminal research, formal education, and rigorous training to properly equip the future United States Department of Defense and public sector cyber workforce in the disciplines of intelligence, information operations, and cyber domains.

CCW's objective is to earn recognition as the premier Center for Excellence in Cyber Warfare and Academic Excellence in Research.

B. KEY STAKEHOLDERS

Organizational theory elucidates that the goals and activities of an enterprise determines its organizational structure (Bothamley, 2002). The agency Program Managers and Service Components specified below influence the strategic learning of the CCW wherein coordination, cooperation, and the transferability of knowledge across multiple levels enables and supports the CCW's stated mission and its ability to discover, explore, and educate to emergent technology in the cyber environment.

1. Director of National Intelligence (DNI)

Among other functions, the DNI is:

> Head of the Intelligence Community (IC), overseeing and directing the implementation of the National Intelligence Program and Policy, and acting as the principal advisor to the President, the National Security Council, and the Homeland Security Council for intelligence matters related to the National Security. Working together with the Principal Deputy DNI (PDDNI) and with the assistance of Mission Managers and four Deputy Directors, the Office of the DNI's goal is to effectively

> integrate foreign, military, and domestic intelligence in defense of the homeland and of United States interests abroad. (Director of National Intelligence Mission Statement, 2010)

Currently, 16 intelligence agencies fall under the purview of the DNI. Each intelligence activity is responsible for a particular intelligence discipline - open source intelligence (OSINT), human intelligence (HUMINT), measurement and signals intelligence (MASINT), imagery intelligence (IMINT), geospatial intelligence (GEOINT), and signals intelligence (SIGINT). Collection techniques utilized by each of these agencies varies slightly therefore voluntary pooling of data and information from these agencies supports information dominance initiatives by providing a more comprehensive picture of the current battle space. This in turn reduces duplication of effort and allows for more efficient tasking of available resources.

To elucidate this point, Table 1 derived from congressional testimonies, mission statements, and known capabilities, provides estimates on each agency's current processes and technologies and their ability to sustain cyber focused operations. On a scale of 1 signifying the low end and 5 at the high end, the ratings convey the relevance and progression of current capabilities with respect to cyber intelligence gathering.

U.S. Intelligence Community	Est. Cyber Capabilities	Current Cyber Role	Future Cyber Role
National Security Agency (NSA)	4.1	5.0	5.0
Central Intelligence Agency (CIA)	4.0	3.9	4.6
Air Force ISR Agency	4.0	3.0	4.0
Defense Intelligence Agency (DIA)	4.0	3.5	4.2
Director of National Intelligence (DNI)	4.0	3.9	4.6
Army Military Intelligence (MI)	3.9	3.0	3.5
Office of Naval Intelligence (ONI)	3.8	3.0	3.0
Federal Bureau of Investigation (FBI)	3.8	3.5	4.5
Marine Corps Intelligence Activity (MCIA)	3.7	2.0	3.0
Office of Intelligence and Counterintelligence (OICI)	3.7	3.0	3.5
Office of Intelligence and Analysis (I&A)	3.6	3.0	3.5
Bureau of Intelligence and Research (INR)	3.6	3.0	3.5
Department of Treasury – Office of Terrorism and Financial Intelligence	3.5	3.0	3.0
National Geospatial-Intelligence Agency (NGA)	3.0	2.0	3.0
National Reconnaissance Office (NRO)	3.0	2.0	3.0
Coast Guard Intelligence (CGI)	3.0	2.5	3.0
Drug Enforcement Agency (DEA)	2.0	2.0	3.0

Table 1. Cyber Intelligence Capabilities (From Technolytics, 2009)

2. Department of Defense (DoD)

The responsibilities and oversight of the national cyber mission sets is enabled by multiple service elements and specific agencies identified in Figure 2.

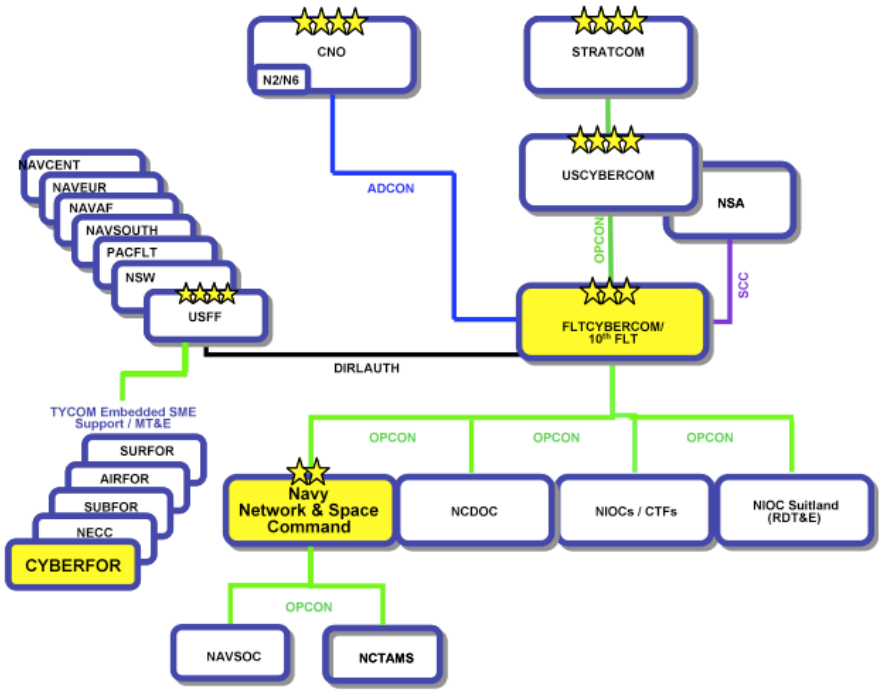

Figure 2. Organizational Chart (From IP Symposium, 2010)

a. Chief of Naval Operations (CNO)

In his administrative capacity, the CNO is:

> Responsible to the Secretary of the Navy (SECNAV) for the command, utilization of resources, and operating efficiency of the operating forces of the Navy and of the Navy shore activities assigned by the Secretary. (CNO Mission Statement, 2010)

From a cyber perspective, direction provided by the CNO included merging of the Chief of Naval Operations (OPNAV) N2/N6 staff to enable integration and innovation of war fighting capabilities, establishment of United States Fleet Cyber Command/10th Fleet to handle operational cyber requirements, realignment of Naval Network Command (NAVNETWARCOM) for execution of network and space

operations, and establishment of Cyber Forces Command (CYBERFOR) to manage manning, training, and equipping requirements as depicted in Figure 2.

b. National Security Agency/Central Security Service (NSA/CSS)

NSA/CSS is the lead defense agency for SIGINT related operations within the DoD and additionally is:

> The U.S. Government (USG) lead for cryptology, and its mission encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) activities. The CSS conducts SIGINT collection, processing, analysis, production, and dissemination, and other cryptologic operations as assigned by the Director, NSA/Chief, CSS (DIRNSA/CHCSS). (NSA/CSS Mission Statement, 2010)

As depicted earlier in Table 1, NSA scored high marks in its current capabilities and as such will remain the most likely organization to lead national cyber related missions. That being said, forging a strong relationship via the resident NSA/CSS Chair addressed in Chapter II Section C will ensure the CCW focuses on research, training, and education pertinent to current and future requirements.

c. United States Cyber Command (USCYBERCOM)

The mission of USCYBERCOM is:

> To coordinate computer network defense and direct U.S. cyber attack operations. (USCYBERCOM Mission Statement, 2010)

Referencing Figure 3, the establishment of USCYBERCOM bears with it the formation of a dual-hatted position. On June 2010, GEN Alexander, the incumbent director of the National Security Agency was appointed Commander for USCYBERCOM operations. Based on this construct, under Title 10 of the U.S. code GEN Alexander will direct actions that pertains to military cyber operations and under Title 50 of the U.S. code he additionally has responsibility for intelligence operations as it pertains to collection and analysis. While concerns have been raised on the political and

legality issues of closely tying the means and ways together, it increases the breadth of intellectual and research opportunities the U.S. and institutions such as NPS gains in the realm of information dominance.

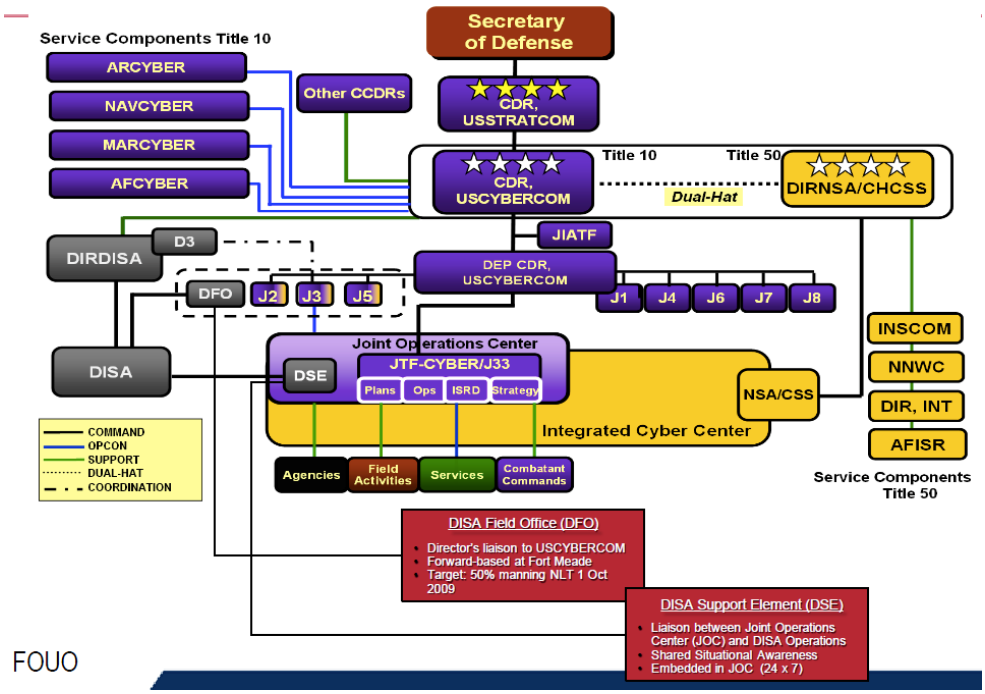

Figure 3. USCYBERCOM Organization (From Van Houten, 2010)

d. United States Fleet Cyber Command (FLTCYBERCOM)

FLTCYBERCOM is the operational arm of the U.S. Navy cyber mission with responsibility:

> To direct Navy cyberspace operations globally to deter and defeat aggression and to ensure freedom of action to achieve military objectives in and through cyberspace; to organize and direct Navy cryptologic operations worldwide and support information operations and space planning and operations, as directed; to direct, operate, maintain, secure, and defend the Navy's portion of the Global Information Grid; to deliver integrated cyber, information operations, cryptologic, and space capabilities; and to deliver global Navy cyber network common cyber operational requirement. (FLTCYBERCOM Mission Statement, 2010)

e. United States 10th Fleet (C10F)

Co-located with FLTCYBERCOM, Tenth fleet controls the operational forces that support the Navy cyber mission of:

> Serving as the Number Fleet for FLTCYBERCOM and exercise operational control of assigned Naval forces; to coordinate with other naval, Coalition, and Joint Task Forces (JTF) to execute the full spectrum of cyber, electronic warfare, information operations, and signal intelligence capabilities and missions across the cyber, electromagnetic, and space domain. (Tenth Fleet Mission Statement, 2010)

Figure 4 details the key operational and geographical areas to which CCW can align ECE Cyber and EW certificate and degree programs. To sustain the cryptologic, network operations (NETOPS), computer network operation (CNO), and information operations functionalities CCW can provide graduate level research and education focused on SIGINT; cyber; space; information operations (IO); electronic warfare (EW); networks; computer systems; digital communications; signal processing; and guidance, navigation, and control.

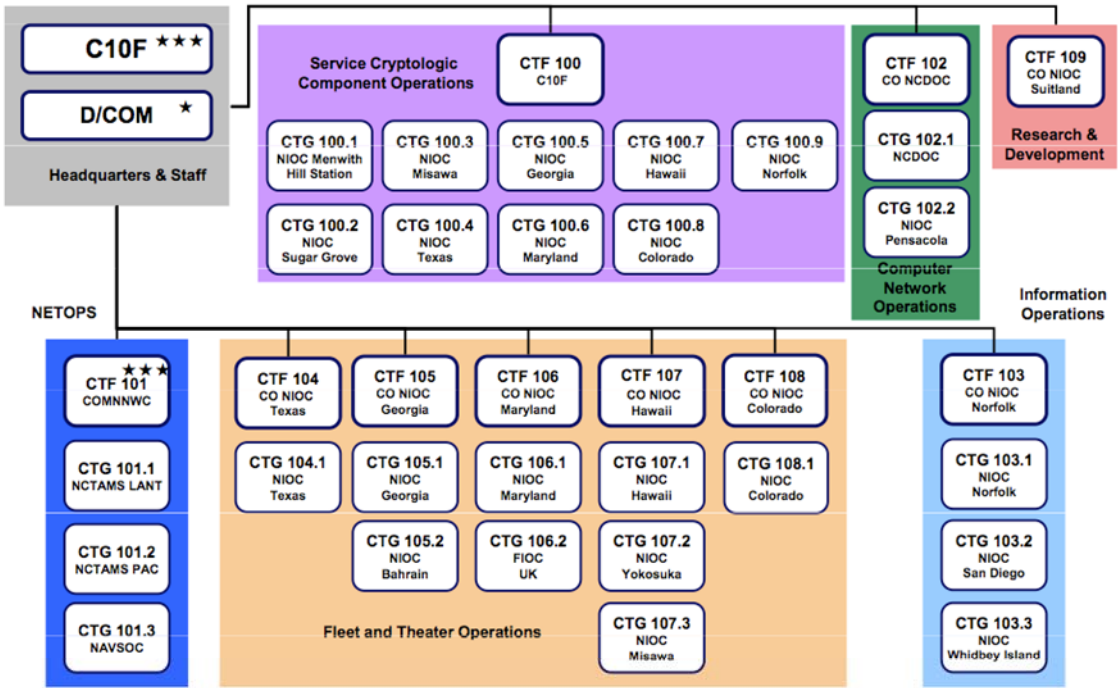

Figure 4. C10F Task Organization (From C10F, 2010)

3. Department of Homeland Security (DHS)

The mission of DHS is three-fold:

> (1) To lead the unified national effort to secure America; (2) prevent and deter terrorist attacks and protect against and respond to threats and hazards to the Nation; and (3) secure our national borders while welcoming lawful immigrants, visitors, and trade. (DHS Mission Statement, 2010)

In this respect, CCW can further its strong ties with DHS and the NPS Center for Homeland Security and Defense (CHDS) by promoting educational opportunities and training programs that support the overarching National Strategy to Secure Cyberspace and by furthering research initiatives aimed at reducing vulnerabilities of national and military infrastructures.

Based on more recent dialogues with DHS, CCW will respond with an interdisciplinary proposal for certificates that address the roles and competencies outlined in the IT Essential Body of Knowledge (EBK) document dated September 2008 (Knorr, 2010). The IT Security EBK is a document developed by the Department of Homeland Security National Cyber Security Division (DHS-NCSD) that offers an overarching document that links competencies and functional perspectives to IT security roles filled by personnel in both public and private sectors. The potential benefit the EBK brings is two-fold – (1) it articulates IT functions in a more context-neutral format and language and (2) provides content that facilitates efficiencies in academic curricula and related activities. To ensure the EBK remains relevant and applicable to the current environment it is maintained as a living document with revisions incorporated every two years. Of the 14 competency areas identified in the EBK, the ECE department will focus on the following:

- **Data Security—**principles, policies, and procedures necessary to ensure the confidentiality, integrity, availability, and privacy of data in all forms of media. Terms associated with data security include—access control, electronic commerce, firewall configuration, steganography, etc.

- **Digital Forensics—**acquiring, validating, and analyzing electronic data to reconstruct events related to security. Terms associated with digital forensics include—cyber laws/guidelines/policies, e-discovery, network forensics, network monitoring, etc.
- **Network and Telecommunications Security**—principles, policies, and procedures involved in ensuring the security of basic network and telecommunications services and data, and maintaining the hardware layer on which it resides. Terms associated with network security include—network segmentation, encryption technologies, defense in depth, networking models and protocols, etc.
- **System and Application Security**—principles, policies, and procedures pertaining to integrating information security into an IT system or application during the system development life cycle (SDLC). Terms associated with system and application security include—security testing and evaluation, configuration management, secure coding, secure system design, etc. (DHS, 2008)

4. National Geospatial-Intelligence Agency (NGA)

NGA provides key geospatial assets to support the U.S. cyber mission. As its mission statement professes:

> NGA provides timely, relevant, and accurate geospatial intelligence in support of national security objectives. "geospatial intelligence" (GEOINT) is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial (e.g., mapping, charting, and geodesy) information. (NGA Mission Statement, 2010)

Through NGA, CCW gains access to GEOINT products obtained from standard spectral imagery coupled with active sensing technologies such as synthetic aperture radar (SAR), light detection and ranging (LIDAR) sensors, and imagery derived MASINT to develop algorithms, tools and data exploitation processes that support the cyber mission sets of advanced geospatial intelligence.

5. Defense Intelligence Agency (DIA)

> DIA's strategy focuses on the core mission areas of collection, analysis, and information services and management and essential enabling and

> support functions. The strategy seeks—(1) first and foremost, a skilled workforce with the attributes and abilities required to meet today's requirements and future challenges; (2) innovative and integrated collection strategies and capabilities; (3) rapid transformation of information to knowledge through responsive and cogent analysis; and (4) state-of-the-practice information management to exploit the power of information technology. (DIA Mission Statement, 2010)

DIA is the primary source for subject matter experts (SME) that support the scientific and technical analysis of foreign military weapons programs. CCW can leverage this expertise and the all source analytic products it produces to better understand foreign military capabilities, particularly in the cyber domain.

6. Central Intelligence Agency (CIA)

> CIA is the nation's first line of defense. CIA accomplishes what others cannot accomplish and go where others cannot go. CIA carries out their mission by—(1) collecting information that reveals the plans, intentions, and capabilities of our adversaries and provides the basis for decision and action; (2) producing timely analysis that provides insight, warning, and opportunity to the President and decision makers charged with protecting and advancing America's interests; and (3) conducting covert action at the direction of the President to preempt threats or achieve U.S. policy objectives. (CIA Mission Statement, 2010)

CCW can leverage CIA expertise on matters pertaining to the national security policy and laws to ensure that CCW science and technology research initiatives and capabilities follow the path of emergent technology.

7. National Reconnaissance Office (NRO)

The NRO provides highly classified resources in support of the U.S. cyber mission. It is:

> A joint organization engaged in the research and development, acquisition, launch, and operation of overhead reconnaissance systems necessary to meet the needs of the Intelligence Community and of the Department of Defense. The NRO conducts other activities as directed by the Secretary of Defense and/or the Director of National Intelligence. (NRO Mission Profile, 2010)

NRO manages all data collection from national satellite systems and airborne platforms. CCW can tap into this resource to further research initiatives in the planned Cross-Domain cyberspace laboratory.

8. Academia/Research Institutions

a. NPS Information Dominance Sponsored Through Cebrowski Institute

The Cebrowski Institute (CI) serves as the Cross-Discipline Research Institute responsible for the establishment of an overarching framework to align affiliated NPS research centers with OPNAV instructions that elucidates consolidation of the Information Dominance Corps officer communities under a single 18xx series of designators and integration of enlisted and civilian counterparts as well (CNO, 2010).

Figure 5 depicts a notional view of extant NPS graduate programs functioning in parallel with associated research centers and how NPS will leverage its multifaceted environment to execute the NPS cyber mission in accordance with higher directives pertaining to cyberspace operations. CCW has aligned itself with CI in support of a cross campus multi-disciplinary approach to cyber focused graduate education and research.

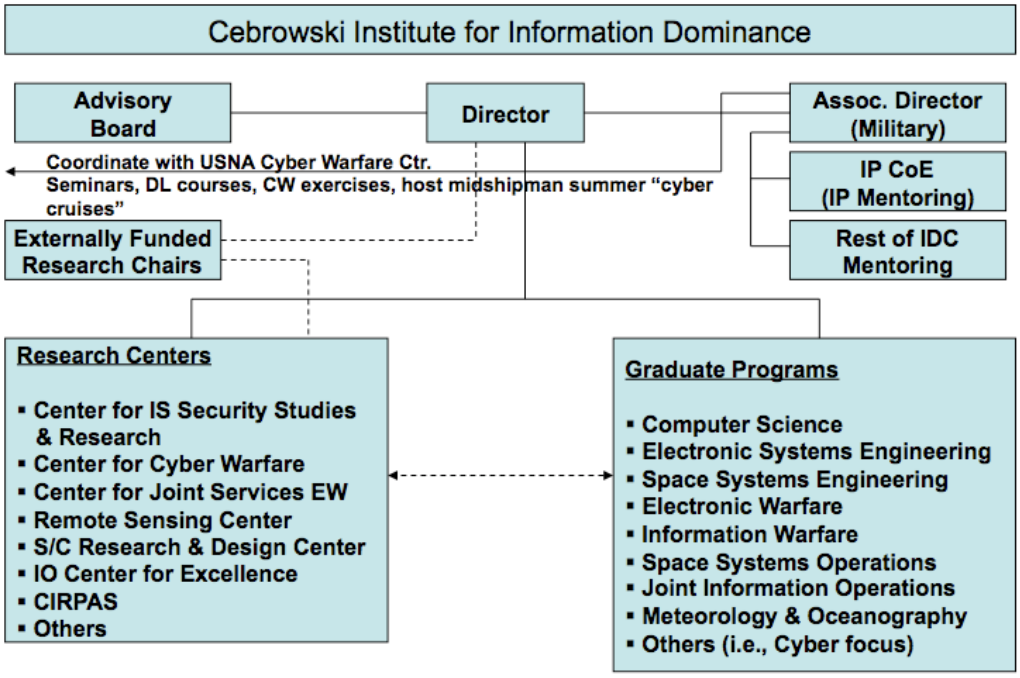

Figure 5. Cebrowski Institute for Information Dominance (From Knorr, 2009)

Additionally, Cebrowski Institute views information dominance, information assurance (IA) and cybersecurity from four perspectives:

- Capability for information gathering, sensing, policies development, deciding, and coordinating in the areas of information, intelligence, counterintelligence, human derived information, and meteorology and oceanography.
- Capability of dominating over enemies who appears as self-organizing autonomous networks.
- Capability for distributing information to operational forces of such quality that the commander's intent doctrine can be implemented reliably.
- Superior performance in these areas is critical to war-fighting capabilities, both in defense and attack.

CI's stated vision in this case, perfectly aligns with the Navy concept of information dominance, wherein every platform is a sensor that is networked so information can be used to achieve decision superiority thus enabling the tactical advantage.

b. United States Naval Academy (USNA) Cyber Warfare Center

USNA will address similar cyber requirements and concerns. Its mission statement aligns perfectly with that of the CCW, namely:

> (1) To enhance the education of midshipmen in all areas of cyber security and operations; (2) to facilitate the sharing of expertise and perspectives in cyber-enabled technologies from across the Yard; (3) to provide a streamlined means of identifying priorities; to enhance inter-disciplinary research; and (4) to disseminate information, harmonize efforts, and shape a common framework for related cyber-enabled mission efforts. (USNA CWC Mission Statement, 2010)

Current course offerings include the areas of networks, advanced networks, information assurance, advanced information assurance, cryptography, and digital forensics. NPS CCW can leverage USNA cyber warfare center laboratory facilities and enable midshipman cross decking by strongly linking USNA cyber interests with ongoing NPS research initiatives through summer "cyber cruises."

c. University Partnerships

Members of U.S. Congress have identified ten emergent cyber/Multi-INT universities, namely—University of Southern California (USC) Viterbi, New Mexico State University, Texas A&M, Utah State University, University of Houston, University of Texas El Paso, Arizona State University, University of Washington, University of Texas San Antonio, and Colorado School of Mines that can spearhead the educational path and assist OPNAV N2/N6 in fostering academic and research ties and serve as breeding grounds to grow the next generation of cyber/Multi-INT warriors. Furthermore, NPS CCW has extended an outreach program with USC Viterbi, where students upon acceptance, will be employed as CCW interns and/or research assistants for a period of six months under their cooperative education work phase.

9. Research and Education Sponsors

Resources such as National Science Foundation (NSF) and House Bill 4061 "Cyber Security Education" can provide for necessary funding to pioneer new research and education initiatives within the CCW.

NSF is:

> An independent federal agency created by Congress in 1950 'to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense…' With an annual budget of about $6.06 billion, NSF is the funding source for approximately 20 percent of all federally supported basic research conducted by America's colleges and universities. (NSF Mission Statement, 2010)

C. CENTER FOR CYBER WARFARE (CCW) ORGANIZATION

CCW's primary focus is the detection and prevention of network attacks. Figure 6 depicts the CCW organizational concept and defines key CCW staff and their corresponding responsibilities.

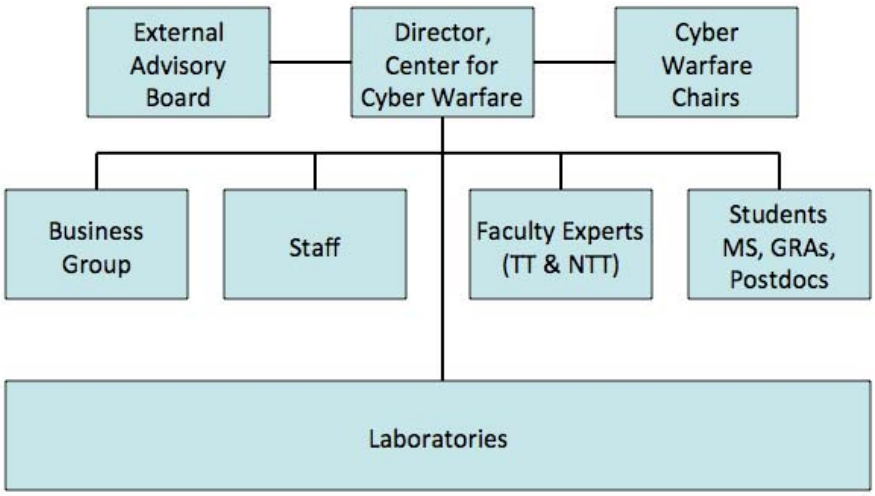

Figure 6. Cyber Center Concept (From Knorr, 2010)

1. **CCW Director**. Serves as Chair on the Executive Committee for CI. The CCW Director will be selected from within the faculty of the ECE Department, and will have an established reputation in the CCW subject area. Eligibility criteria as defined in NAVPGSCOLINST 3900.2, requires that the Director be tenure track (TT) with eligibility for non-tenure track (NTT) given under special circumstances. As the central authority for the operation and maintenance of the CCW, the CCW Director has the following responsibilities:

- Provide CCW's strategic vision of its overall mission and operation to prospective students and faculty members.
- Inform the Provost, Dean of Research, and ECE chair on all operational and administrative requirements of the CCW.
- Submit and oversee announcements and/or calls for employment to include staff positions, TT and NTT faculty, and graduate research assistants to ensure employment of candidates who can effectively support CCW initiatives.
- Maintain oversight on all student and faculty research within the CCW and ensure its relevance to current national security and technical objectives.
- Monitor student and faculty research conducted within the CCW and associated laboratories in accordance with stated NPS business/academic best practices.
- Collaborate with the directors of CI's various unclassified and classified research laboratories, and fully coordinate CCW research with similar efforts being conducted in various NPS research facilities.
- Ensure availability of resources to appropriate users at all times.
- Ensure all research initiatives are handled at the appropriate level of classification, and within the appropriate facility.
- Ensure the physical security of equipment and information stored within unclassified and classified CCW facilities.
- Assist in shaping the level of effort and funding requirements for research tasks by collaborating with various sponsors and research partners.
- Provide definitive guidance and assistance in developing solicitation and funding requests from current or potential research sponsors.
- Appropriate fund expenditures provided to the CCW for both research and non-research related purposes.

- Provide oversight on the fund expenditures allocated to the CCW for material requisitions and travel.
- Inform associated sponsors and research partners on the expenditure of research funds and the status of research efforts conducted within the CCW.
- Coordinate and supervise the visitation of sponsors, partners, and other interested guests in the CCW.
- Direct the CCW Associate Director in the daily maintenance of material, logistical, security, technical, procedural, and personnel issues within the CCW.
- Conduct periodic performance appraisals for CCW employees, as required.
- Collaboration with other agencies at multiple classification levels requires that Director meet applicable investigative, security clearance directives, and requirements.

2. Resident NSA/CSS Chair. At present, a resident NSA/CSS chair has not been identified. If and when the position is filled, the Chair will serve as the primary liaison between NPS and the DoD cyber community. In this respect, the Resident NSA Chair has the following responsibilities:

- Serve on the external advisory board and ensure continued alignment of CCW with future U.S. cyber initiatives.
- Provide guidance to the CCW on current and projected DoD cyber related technology and operational issues.
- Assist the CCW Director in locating potential sponsors and establishing research partnerships with the greater intelligence community.
- Monitor and assist the CCW Director in keeping appraised of the research efforts conducted within the various unclassified/classified laboratories, and maintaining the focus of these efforts on national SIGINT objectives.
- Assist in shaping the level of effort and funding requirements for research tasks by collaborating with various sponsors and research partners.
- Appropriate fund expenditures provided to the CCW from the DoD cyber community and diverse sponsors.
- Provide guidance and assistance in proper classification of research initiatives, and the migration of such research into appropriate classified facilities.

- Collaboration with other agencies at multiple classification levels requires that the Chair meet applicable investigative, security clearance directives, and requirements.

3. **CCW Associate Director**. The Associate Director will principally be a NPS military faculty member, with expertise in specific communications subjects, appointed from any of the information dominance associated academic departments to assist the CCW Director as necessary. The Associate Director has the following responsibilities:

   - Ensure information and knowledge received from CCW Director is delivered to the proper audience and addressed as required.
   - Coordinate efforts with analogous military academic institutions (i.e., USNA Cyber Warfare Center, AFIT) in hosting symposiums, collaborative exercises, and cross-deck training.
   - Coordinate CCW research efforts with other unclassified and classified NPS laboratories or facilities.
   - Serve as the liaison for military students and all matters pertaining to such.
   - Provide requisite IDC mentoring through the various Centers of Excellence both while on station and upon departure from NPS through follow-on training and distance learning opportunities.

4. **CCW Business Group**. NPS CCW presents itself as a unique institution that strives to increase the combat effectiveness of its forces through graduate education programs while enhancing the security of the United States. To sustain academic education and foster continued research, the Business Group has been tasked with the following responsibilities:

   - Define and coordinate long and short-range financial plans and programs.
   - Research and accentuate innovative learning technologies, pedagogy, and practices to elicit and provide for enduring proficiency of strategic cyber principles.
   - Assist the CCW Director in locating potential sponsors and establishing research partnerships with civilian industries.
   - Develop and maintain strong working relations with combatant commanders (COCOM), type commanders (TYCOM), OPNAV organizations, Naval Warfare Development Command (NWDC), industry, and other organizations and agencies such as NSA, NRO, and DHS.

- Develop and maintain longstanding partnerships with other colleges and universities, business and industry (i.e., National Science Foundation), government, and the international community.
- Recruit and maintain a diversified academia to support CCW mission and overarching NPS mission sets.
- Ensure seamless integration of graduate students with faculty on advanced concept and research initiatives.

5. **CCW Laboratory Manager**. The CCW proposes six research laboratories focused on the different aspects of network operations and security. The laboratories, which function at different levels of classification, have been identified as those with a concentration on computer network attack (CNA), communications research, computer network operations (CNO), Honeynet, cross-domain cyberspace, and mobile broadband wireless. The CCW Laboratory Manager is tasked with the following responsibilities:

- Monitor and ensure operability of CCW server farm and associated equipment.
- Maintain accurate documentation of all CCW major expenditures, equipment purchases and deliveries, and minor property inventory.
- Provide support services to include that of control and computer systems, communications (including networking), data acquisition, physical measurements, electro-mechanical systems, telemetry, mobile radio, and signal analysis and generation equipment.
- Provide administrative level support to faculty and ensure best effort in providing curricula laboratory requirements to include procurement of necessary hardware equipment, software applications and systems, and/or providing recommendation or resolution when current technology or lack of funding precludes such.
- Oversee day-to-day operations and maintenance of all CCW laboratory and server spaces.

6. **CCW Faculty**. Composed of Tenure Track (TT) and Non-Tenure Track (NTT) faculty. Primary responsibilities include but are not limited to:

- Conduct sponsored, externally funded research.
- Instruct or facilitate resident, synchronous, and asynchronous distance based learning via video tele-education (VTE) and/or computer network resources.

- Serve as an advisor to thesis students.
- Participate in both internal and external service activities.
- Assist in building the network engineering and cyber research program through collaboration between department faculty and solicitation of financial support for research initiatives.

7. **CCW Student Technical Directors**. Student technical directors will be selected from the student body based on their academic performance, efficient managerial skills, knowledge of cyber warfare and associated communications systems, and more importantly, their aggressive leadership and broad operational experience. The CCW Student Technical Director will play a major role in the daily operation of the CCW laboratories and must be forward thinking and proactive. The amount and scope of administrative and operational responsibilities within the CCW may eventually necessitate that more than one Student Technical Director be appointed. The responsibilities of the CCW Student Technical Director include:

- Support the CCW Associate Director, the academic chairs, and the Resident NSA/CSS Chair in all matters pertaining to the efficient operation, maintenance, and requirements of the CCW facilities.
- Coordinate, supervise, and assist students and faculty in the daily operation and maintenance of the CCW facilities, equipment, and other material.
- Assist in shaping the level of effort and funding requirements for research tasks by collaborating with various sponsors and research partners.
- Coordinate and assist in the identification of material, logistical, security, technical procedural, and personnel requirements within the CCW, and such requirements between the CCW and other cooperating NPS laboratories.
- Assist CCW laboratory manager in maintaining accurate documentation of all CCW major expenditures, equipment purchases and deliveries, and accountability of minor property inventory.
- Assist in the identification of potential candidates for his or her relief as the CCW Student Technical Director.

8. **Research Sponsors.** To sustain CCW's strategic cyber vision and research initiatives requires material and/or financial support from various military,

government, and commercial sponsors. Unreserved participation of these sponsors is crucial for maintaining the focus of CCW research initiatives on the more technical issues and cyber challenges that can potentially affect our nation's networks and critical infrastructures. Equally important is that CCW conduct the most advanced research possible and maintain its "first mover" advantage through adoption of emergent technology. First movers in this case would be the early entrants to market that have the opportunity to build capacity and knowledge base to discover and exploit unknown areas in the cyber domain. (Ketchen, Snow, & Hoover, 2004) Establishment and sustainment of long term relationships is mutually beneficial to CCW and its associated sponsors in that research initiatives can exploit cyber issues using available pooled resources and output processes or resultant techniques that can further enhance situational awareness and protection of their respective cyber infrastructures.

Prospective research sponsors should establish relationships via a standard NPS research proposal, an Educational Partnership Agreement (EPA) and/or Cooperative Research and Development Agreement (CRADA), Memorandum of Agreement (MOA), or Memorandum of Understanding (MOU) that provides the CCW with a detailed description of the specific joint technical objectives that is mutually beneficial to all parties concerned and promotes advancement of their scientific capabilities and knowledge. Additional support should be encouraged and may include:

- Specification of mission objectives and reporting requirements.
- Direct funding for research related material, labor, and travel.
- Pooling of resources such as the transfer of excess equipment to the custody of the CCW and/or purchase of new hardware and other research material.
- SME on-site/off site mentorship.
- Awards for student research grants or fellowships.
- Use of the sponsor's indigenous research facilities.
- Access to and use of proprietary hardware and software.
- Sponsorship and coordination of student experience tours.

D. OPERATIONAL OBJECTIVES

NPS provides a unique graduate environment where as an Echelon II command it serves the capacity both as an administrative and an operational unit. In its administrative capacity, NPS provides a medium for:

> Collaboration and building partnerships with other colleges, universities, business and industry, government, and the international community. Furthermore, it fulfills the requirements of encouraging relevant and meritorious research while enabling the intellectual capital of NPS civilian and military faculty. (NPS Mission Statement, 2010)

From the standpoint of its operational function – *NPS exists for the purpose of increasing the combat effectiveness of the Navy and Marine Corps and other associated services.* As a military centric institution, NPS fulfills its operational relationship to the President of the United States (POTUS) and Chief of Naval Operations (CNO) by ensuring that advanced graduate education aligns with extant guidance particularly those policies pertaining to national security. The Comprehensive National Cybersecurity Initiative (CNCI) formally launched January 2008 by President George W. Bush via National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/ HSPD-23) is one such document that forms the foundation from which CCW mission sets are derived.

In accordance with the aforementioned guidance, and to fully align with NPS Information Dominance stated goals, first and foremost, CCW will ensure that its organizational structure complements other CI initiatives allowing for seamless integration and to curtail potential duplication of efforts. The succeeding paragraphs expounds on the specific initiatives that CCW has the capacity to support.

- CCW will collaborate and sustain its extant relationship with its key stakeholders to guarantee that the most pressing issues are addressed. To further enhance its research initiatives, CCW will foster expansion of its repertoire of sponsors and associations to include federal, state agencies, universities, private sector, and international partners interested in meshing cyber related research and development efforts (CNCI 4, 2010).
- CCW will support efforts of increasing situational awareness amongst different cyber operations center by providing long-term research on

cross-domain solutions to ensure that interagency transfer of information both at the unclassified and classified levels transpires seamlessly and securely with minimal threat of compromise by a likely adversary (CNCI 5, 2010).

- CCW will leverage its relationship with key stakeholders identified in Chapter II Section B to properly shape and capture significant facets of a cyber counterintelligence plan for government wide implementation (CNCI 6, 2010).
- CCW will coordinate horizontal integration of research and instructional efforts with related curricula and/or departments to ensure networks and the elements of data integrity, confidentiality, and authenticity are duly safeguarded from penetration, exploitation, and/or acts of cyber aggression (CNCI 7, 2010).
- CCW will fully integrate U.S. Navy's information dominance objectives and forthcoming roadmaps into current and all future courses of instruction. The IDC roadmaps referenced will align and synchronize all navy-related missions and covers the following areas – air dominance, convergence to a single Navy network, cyberspace operations, decision superiority, education, electromagnetic spectrum management, fleet battle management, integrated surface sensors, intelligence, surveillance, and reconnaissance (ISR), maritime ballistic missile defense, maritime domain awareness, spectrum usage, strike command and control, undersea dominance, and unmanned systems. Based on these initiatives, CCW will leverage existing curriculums and resident research facilities to expand its scope and shape a cyber force armed with the requisite knowledge, skill sets, and tools to execute the stated mission tasks (CNCI 8, 2010).
- As an academic institution, CCW can influence the "first mover advantage" by defining potential technological opportunities for study and research and developing long-term strategies for the cyber domain (CNCI 9, 2010).
- NPS represents a very diverse community of U.S. and international military and civilian professionals. As such, CCW can tap into these individuals to better understand "user needs" and utilizing the Defense Acquisition Management System identify emergent technology opportunities and resource requirements to sustain collaborative research in program offices within the field activities of Naval Air Systems Command (NAVAIR), Naval Sea Systems Command (NAVSEA), and Space and Naval Warfare Systems Command (SPAWAR). From the standpoint of deterrence strategy, CCW can leverage resident Naval War College subject matter experts (SME) to develop and further refine policies focused on network offense (CNCI 10, 2010).

- Consistent with guidance derived from the National Strategy to Secure Cyberspace, CCW can further refine the Federal role to include cybersecurity of critical infrastructure to prevent, reduce vulnerability to, and minimize damage and recovery time caused by cyber attacks (CNCI 12, 2010).

E. FUNCTIONS

As referred to earlier, CCW is one of several research centers on the NPS campus that provides related graduate programs that supports the vision of information dominance. CCW's functions are addressed in this section and the succeeding segment defines CCW's specific areas of education and research.

The CCW will meet the above needs and operational objectives by accomplishing a number of specific functions:

- The CCW will serve as the leading facility for NPS students to conduct advanced unclassified/classified research related to communications and information systems, computer and information networks, and media and broadcast systems that support offensive and defensive cyber missions. Research will focus primarily on cyber warfare related initiatives. CCW will additionally coordinate with the Center for Joint Service EW (CJSEW) that has the lead for radar and electronic warfare systems.
- The combined technical knowledge and operational experience students and faculty gain from research conducted within the CCW will align with stated national security objectives and support military mission specific requirements where applicable.
- Faculty associated with the CCW will perform advanced research in their respective fields of study and proactively engage students to support their endeavors.
- Faculty and students will analyze and evaluate specific cyber related tools and cyber domain threats, conduct focused research, and write technical papers and theses on applicable cyber areas of interest. The results of these efforts will provide value added to current and emergent cyber techniques that could potentially initiate national and/or military cyber policy change recommendations.
- The CCW will acquire requisite equipment and corresponding support elements to pursue advanced research functionalities and additionally develop leading edge cyber techniques and tools. This function pertains to

all computers and network equipment, communications hardware and software, and the facilities and personnel support deemed necessary to maintain them.

- The CCW in conjunction with its associated laboratories, will ensure adherence to specific guidelines for circumstances that require migration of sensitive research themes from the unclassified CCW laboratories to NPS's Sensitive Compartmented Information Facility (SCIF), and/or to the laboratory facilities of collaborative research sponsors, for continued studies at higher classification levels.
- The CCW will maintain an independent secure space in the long-term, to directly sustain research efforts that require use of classified media or techniques, alleviating direct impact on allocated resources supporting other NPS research facilities.
- The CCW will proactively lead collaborative research projects with other unclassified and classified laboratories, both at NPS and other various academic, military, and national research facilities. Doing so will ensure most efficient use of available national research resources, research initiatives are structured appropriately to meet the specific requirements, and are mutually beneficial to all research partners.
- The CCW will provide all military and civilian students, irrespective of designator or job description and level of clearance, significant exposure to the unclassified aspects of cyber technology, tools, techniques, and tactics, and promote the awareness of cyber options at the strategic and tactical level.
- The CCW will coordinate both on-site and off-site education opportunities for students, faculty, and other military and civilian personnel to hone their understanding and improve skills required to use the tools available in the CCW and enhance laboratory research as it applies to the cyber domain.
- The CCW will serve as a database repository of unclassified background and technical information. The intent is to support new students who are seeking additional guidance and provide focus on their prospective research areas that will culminate with the completion of a masters' thesis. Relevant research and experimentation initiatives and all master theses will then be compiled into the CCW database repository.
- Students and faculty associated with the CCW will provide solicitations to establish technical and financial sponsorships with the various military and national laboratories, research facilities, and agencies.

- The CCW will help to educate senior visitors and other guests on current cyber issues, tools, and possible vulnerabilities in both commercial off the shelf (COTS) technologies and DoD Intelligence systems, through demonstrations utilizing applicable resources of the CCW and presenting results of studies and analysis conducted in the CCW laboratory.

F. FOCUS AREAS

1. Education

The ECE department currently offers several degree programs namely—Master of Science in Electrical Engineering (MSEE), Master of Science in Engineering Science with a major in Electrical Engineering MSES(EE), Master of Science in Computer Engineering (MSCE), Master of Science in Engineering Science with a major in Computer Engineering MSES(CE), Electrical Engineer, Doctorate (Ph.D.) all of which are research based and Master of Engineering with Major in Electrical Engineering MEng(EE) and Master of Engineering with Major in Computer Engineering MEng(CE) that are course based.

As an example, the MEng (EE) degree with a focus on SIGINT/Cyber/Space Systems is intended for students who are recent BSEE/CS/CE graduates. Special cases wherein a student by virtue of their education and on-the-job experience exhibit capability to likewise specialize in this area of study can also be given due consideration. This coursework-based degree allows practicing engineers to analyze cyber networks, specify characteristics of cyber systems, and demonstrate an understanding of attack and defense cyber systems.

Figure 7 illustrates the typical course of study that awards a Master of Science in Cyber Systems and Operations upon successful completion of curriculum requirements. The requirements would include a regular track equivalent to 4 courses, a deep track of 8 courses and a cyber-focused thesis supported by track courseware as identified in Table 2.

Q1	Cyber Network and Physical Infrastructures (EC3730)	Introduction to Computer Security (CS3600)	Introduction to Cyber Operations (ISxxxx)	Seminar
Q2	Conflict in Cyberspace (DA3105)	Critical Infrastructure Vulnerability Analysis and Protection (CHDS)	Mathematics of Cyber Security (MAxxxx)	Seminar
Q3	Track 1	Track 2	JPME	Individual Study
Q4	Track 1	Track 2	JPME	Thesis Research
Q5	Track 1	Track 2	JPME	Thesis Research
Q6	Track 1	Track 2	JPME	Thesis Research

Figure 7. MS in Cyber Systems and Operations Matrix (From Knorr, 2010)

Tracks in Cyber Operations	**Tracks in Cyber Operations**
IA Professional Certification	Network Engineering
Cyber Security Fundamentals	Information Systems Security Engineering
Cyber Security Offense/Defense	Cyber Warfare
Identity Management	SIGINT and EW
Digital Forensics	Space Systems
Cyber Planning and Targeting	Systems Engineering
Command and Control for Cyber Operations	Trustworthy Systems
Information Operations	
Social Networks	
Mathematics of Secure Communication	**Deep Tracks**
Mathematics of Networks	Cyber System Defender
Critical Infrastructure Defense	Cyber System Hunter

Table 2. Track Course Requirements (From Knorr, 2010)

To satisfy requirements addressed by C10F and other associated organizations, CCW proposes a comprehensive curriculum that covers the general areas of signals intelligence, computer communications, network engineering, information operations systems, and computer network operations to include network defense, surveillance, and attack. The structure of this curriculum in turn provides Electrical Engineering (EE) graduates with the requisite principles, tools, and techniques for application in cyber research, design, development, testing, and evaluation in follow-on tours.

Figures 8 and 9 present a theoretical flowchart of prerequisite coursework and associated curriculum elective that culminates with the completion of 16 units of EC0810 focused on thesis research and submission of a graduate level cyber engineering related thesis. Supporting directives additionally emphasize that other courses may be used in satisfaction of the elective requirement with the advance approval of the Cyber Engineering Academic Associate.

A proposed Cyber Warfare Certification Program with focus on EW, networks, computer systems, digital communications, signal processing, and guidance, navigation and control is additionally derived based on completion of the modules illustrated in the core courses matrix of Figure 8. The target audience would be distance learners through a distributed learning environment provided by Center for Educational Design, Development, and Distribution (CED3).

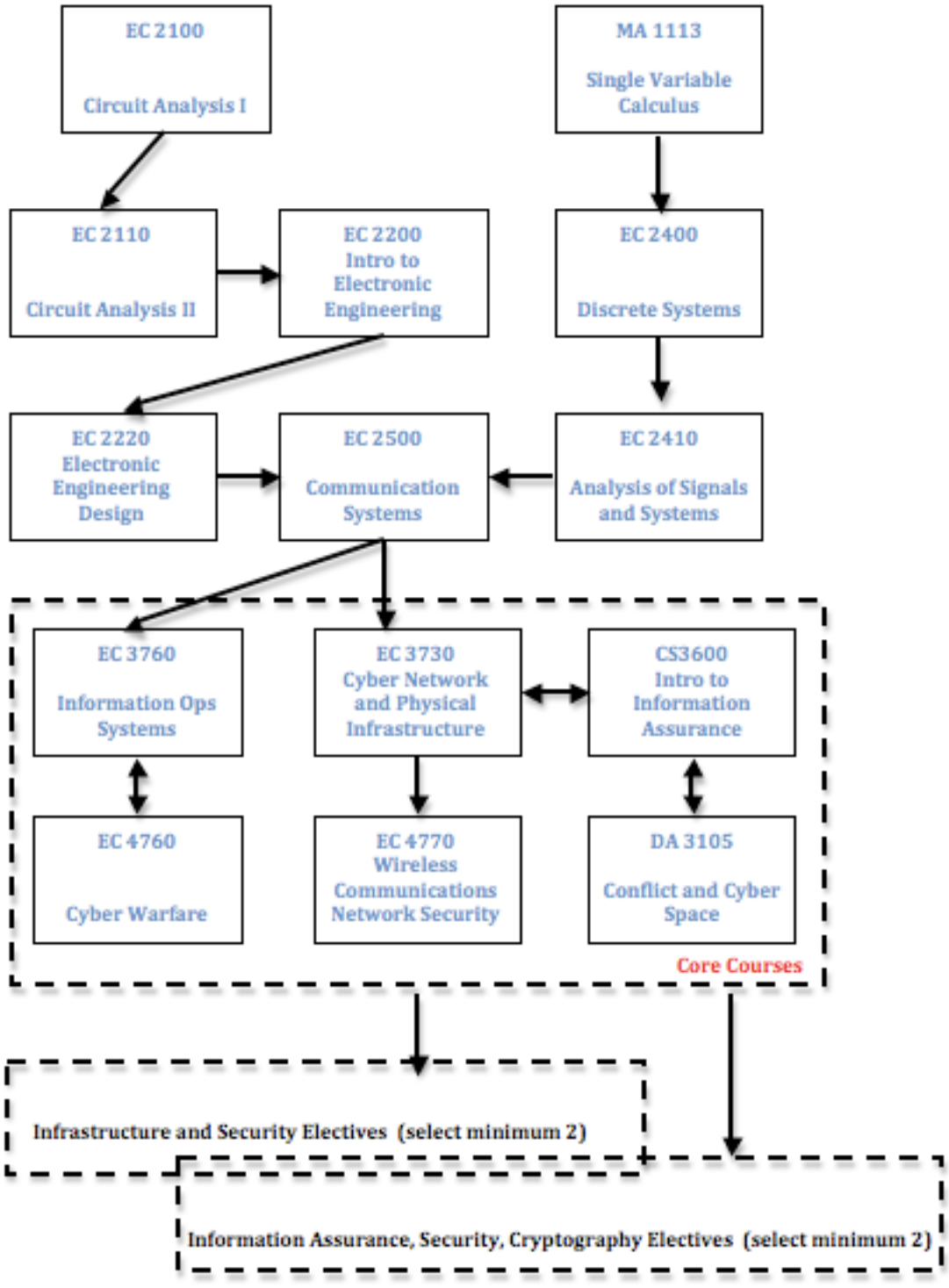

Figure 8. Prerequisite for Cyber Engineering Specialization

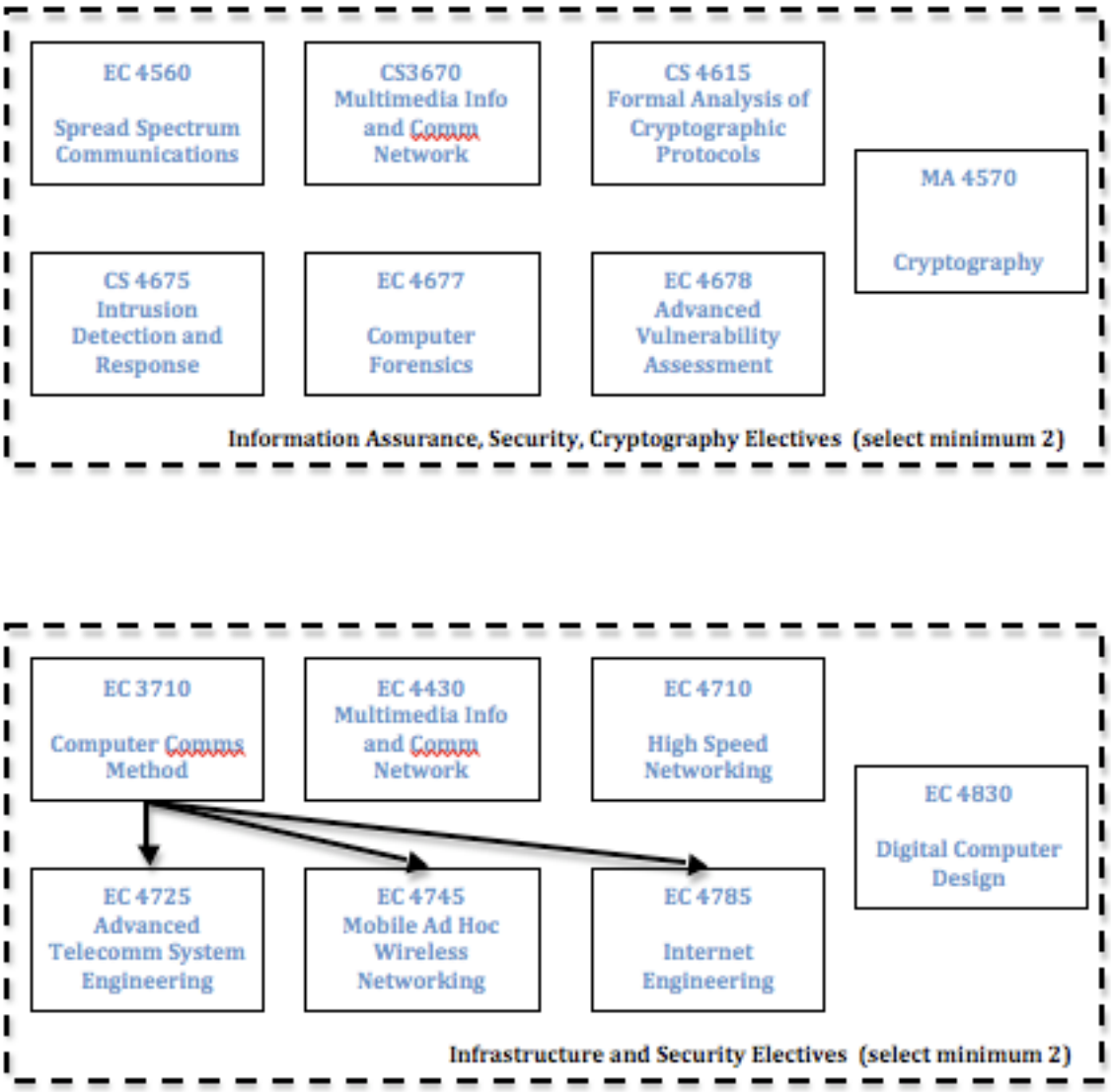

Figure 9. Cyber Engineering Specialization Electives

In addition to the proposed coursework, to assure a minimum level of competency for prospective Cyber Engineers, CCW will incorporate the Information Dominance Corps (IDC) Personnel Qualification Standard (PQS) and NAVNETWARCOM's Job Duty Task as a benchmark tool that focuses on providing an introduction to fundamental principles and the study of specific functional communication, information processing, and intelligence systems.

Upon graduation, based on the Introduction to Fundamental Principles section of the PQS, the student should have the ability to:

- Demonstrate basic understanding of applicable organizational doctrine and regulations.
- Exhibit knowledge of different types of Intrusion Detection System (IDS).
- Demonstrate knowledge of the different types of firewall—security.
- Define maintenance installation requirements for Cryptologic Carry On Programs (CCOP).
- Demonstrate knowledge of circuits in terms of frequency range, type, units on the net, and usage as it pertains to naval communications.
- Define satellite communications principles.
- Explain the rules of engagement (ROE) in reference to computer network attack (CNA), CNA operational preparation of the environment (OPE), computer network defense response action (CND RA).
- Define applicable radio frequency theory terminology, processes, and modulation principles.
- Define all intelligence disciplines and applicability to fusion analysis.
- Define intelligence systems and roles of different collection assets.
- Define IW Electronic Warfare terms.
- Demonstrate IW knowledge of the different types of radar.
- Demonstrate IW knowledge of seeker technology.
- Define and explain meteorological terms and elements.
- Define and explain oceanographic terms and elements.
- Exhibit knowledge of Information Professional (IP) fundamentals.
- Exhibit knowledge of space fundamentals.

Under the Introduction to Systems PQS section, the student should be able to:

- Identify key system components and component parts of communication systems.
- Define purpose and functions of information processing systems.
- Demonstrate the information systems architecture and key system components and component parts (NAVEDTRA 43360, 2010).

Application of these education initiatives perfectly aligns with the roadmap set forth by Director of Total Force Management RDML Robin Braun, which shifts the former 16XX designators knowledge base to a more comprehensive skill set of 1800/Oceanographers, 1810/Information Warfare, 1820/ Information Professional, 1830/Intelligence, 1840/Cyber Warfare Engineer, and 1850/ Cumulative IDC Billets, which utilize information as their main battery to sustain the Navy's vision of information dominance in the fields of ISR, cyber warfare, C2, information and knowledge management (Braun, 2010).

2. Research

The demand for technology that is both evolutionary and revolutionary will likely continue to persist and, as such, requires a roadmap towards a more in depth understanding of near term and long term capabilities. Organizations such as the International Telecommunication Union (ITU) that are responsible for enabling and sustaining global telecommunications through standardization and collaboration; the Federal Communications Commission (FCC) and National Telecommunications and Information Administration (NTIA) that serves as regulatory bodies for non-Federal and Federal allocation for use of the radio spectrum; and the Institute of Electrical and Electronics Engineers (IEEE) charged with management of Internet standards provide the foundation and standards from which CCW will derive both theoretical and applied research in the areas of computer network operations, information operations, signals intelligence, and cyber.

In the field of mobile communications alone, Figure 10 provides a visual indication of the dramatic rise in its penetration among the subscriber base that in turn equates to a sharp increase to data usage and the need for more robust capacity cellular systems coupled with improved spectral efficiency and access technologies. While ITU-Radio Communications and IEEE have provided visions and standards addressing this issue, consortiums such as the Wireless World Research Forum (WWRF), Mobile IT Forum, Future Technology for Universal Radio Environment Project (FuTURE), Next Generation Mobile Communication (NGMC) Forum, 4G Research Cooperation Projects

in the European Sixth Framework Program (FP6), Worldwide Wireless Initiative (WWI), Samsung 4G Forum, and eMobility Technology Platform have each taken the lead in spearheading major 4G initiatives in the areas of network and mobile systems technologies such as ad-hoc networks, quality of service (QoS) and security and encryption techniques; and transmission and access techniques such as Code Division Multiple Access (CDMA), Orthogonal Frequency Division Multiple Access (OFDMA), and Time Division Multiple Access (TDMA) (Prasad & Kim, 2006).

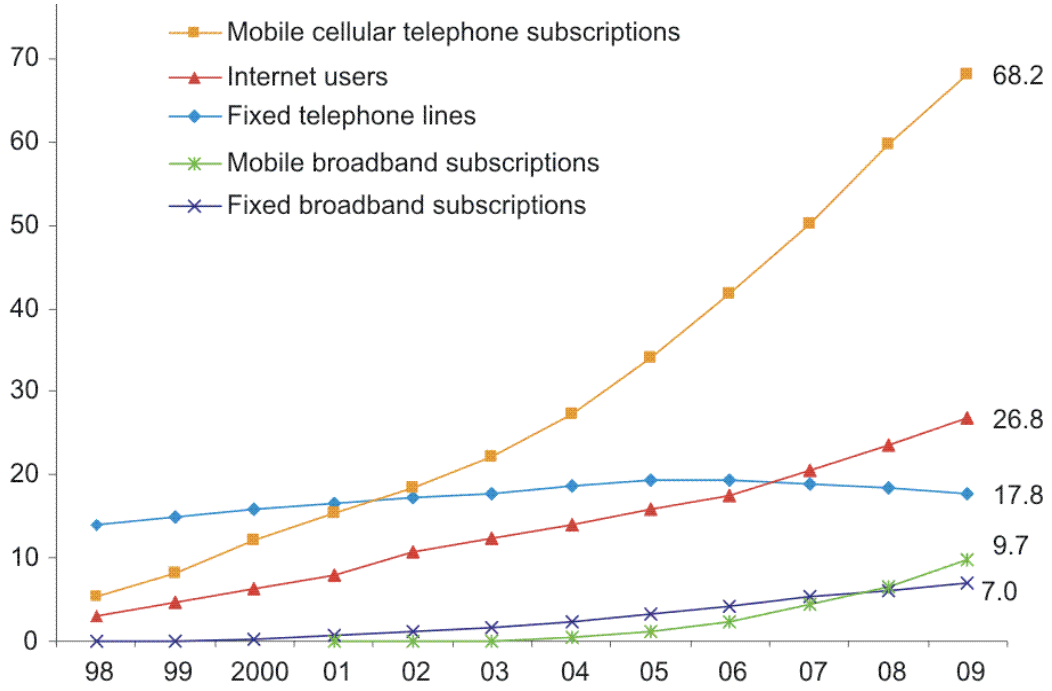

Figure 10. Global ICT Developments 1998-2009 (From ITU, 2010)

Of particular interest right now to the global telecommunications community is the advent of Fourth Generation (4G) technologies particularly that of Long Term Evolution (LTE) and Worldwide Interoperability for Microwave Access (WiMAX). Figure 11 is representative of the current deployment of infrastructure supporting these broadband technologies. Internet connectivity is slowly shifting away from fixed broadband to wireless application due to absence of copper and Digital Subscriber Line (DSL), minimal broadband connectivity and need to sustain economic growth and development. Comparison of both technologies shows analogous performance and

capacity in the 1.5 to 28 MHZ channels. These same emerging broadband standards utilize Orthogonal Frequency Division Multiplexing (OFDM), Internet Protocol (IP), and Multiple-Input Multiple-Output/Beam Forming (MIMO/BF) techniques to exhibit increased efficiency, capacity, and scalability. While WiMAX and LTE are available to the consumer, both have not quite hit the mark in attaining designation as International Mobile Telecommunications (IMT) advanced 4G technology.

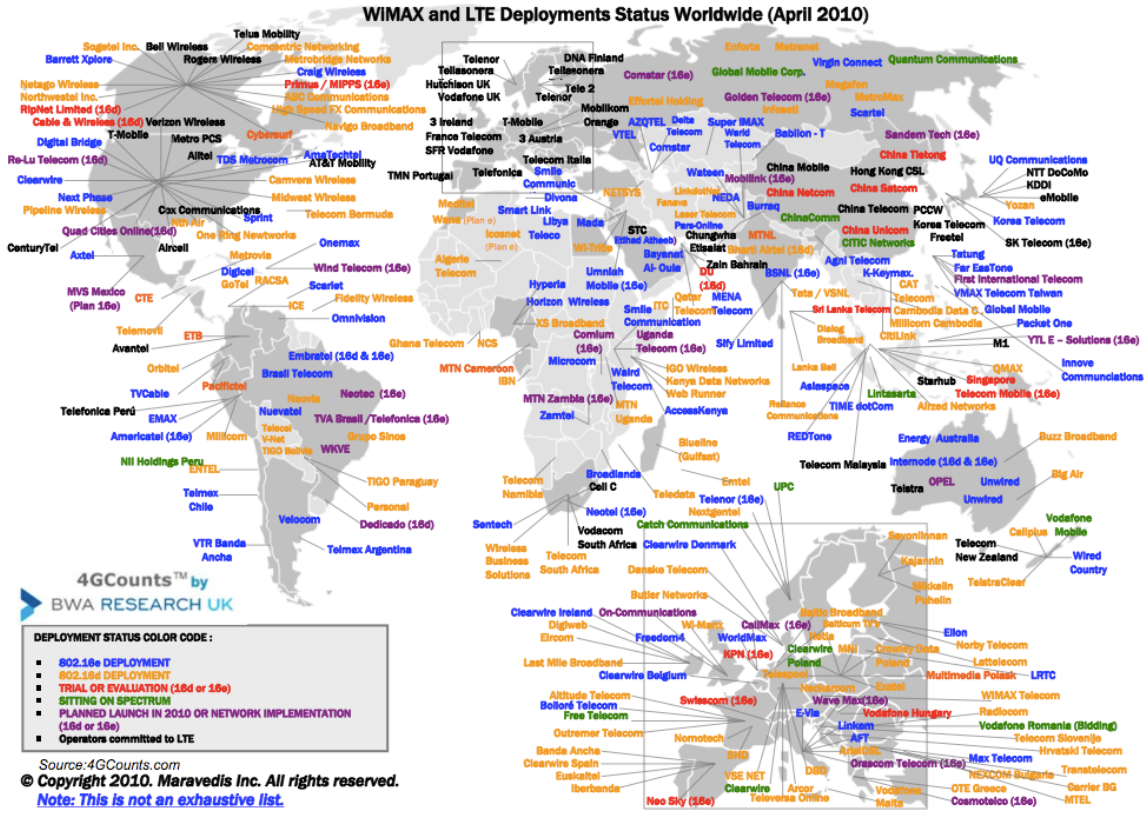

Figure 11. WiMAX and LTE Deployment Status Worldwide (From Maravedis, 2010)

The mere fact that this technology will likely continue to carry out at least for the next five to ten years as other research initiatives take shape for the future generation network known as Broadband Personal Area Network (B-PAN), it is imperative that CCW remains at the forefront in developing and thoroughly understanding LTE and WiMAX. ECE department professor, Dr. McEachen last year presented a brief addressing the threats to mobile wireless device and the path industry is taking to meet

increased wireless broadband requirements. Figure 12 depicts Dr. McEachen's visual representation on the evolution of WiMAX and LTE technologies.

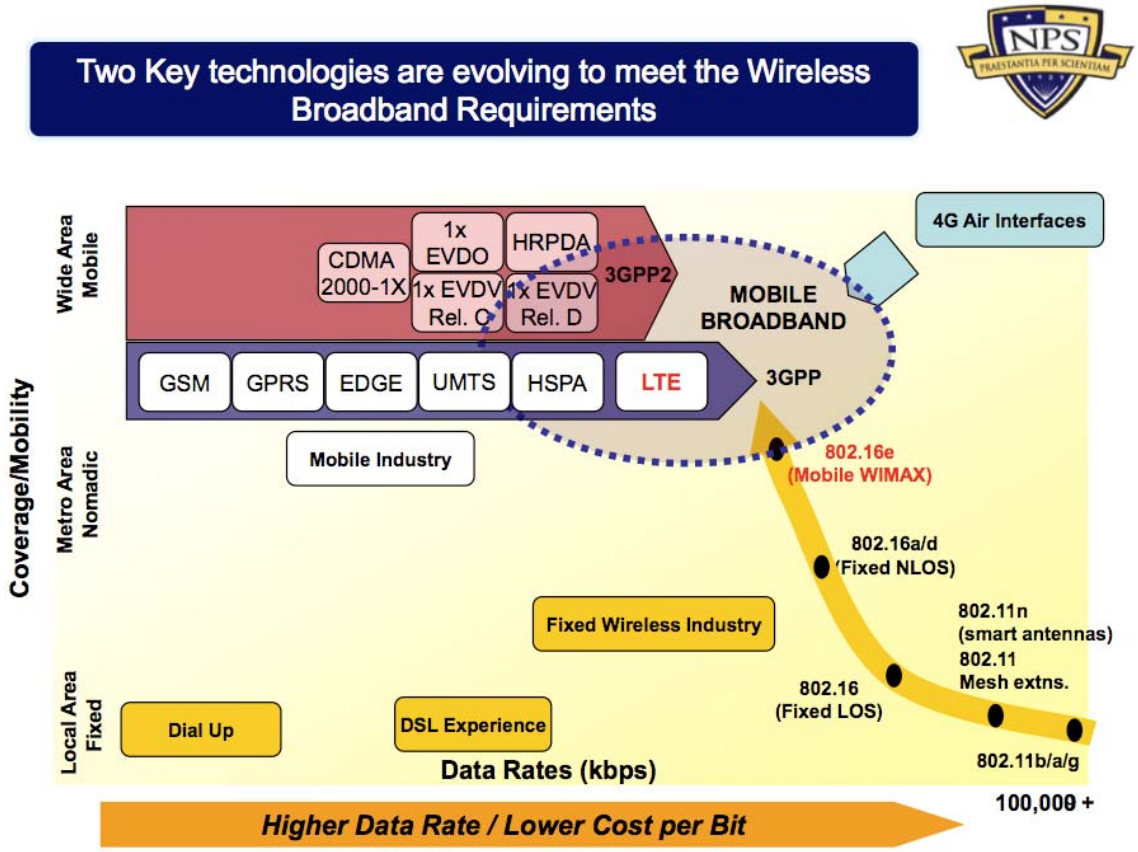

Figure 12. Wireless Broadband Requirements (From McEachen, 2009)

To remain abreast of these potential revolutionary transformations CCW will conduct research of innovative technology and continued development of existing communication technologies utilizing available tools and techniques, modeling, simulation, computer programming and theoretical analyses that will be supported through six specific laboratories illustrated in Figure 13 with documentation of finished research work to find itself in master thesis, dissertations, technical reports, and conference presentations.

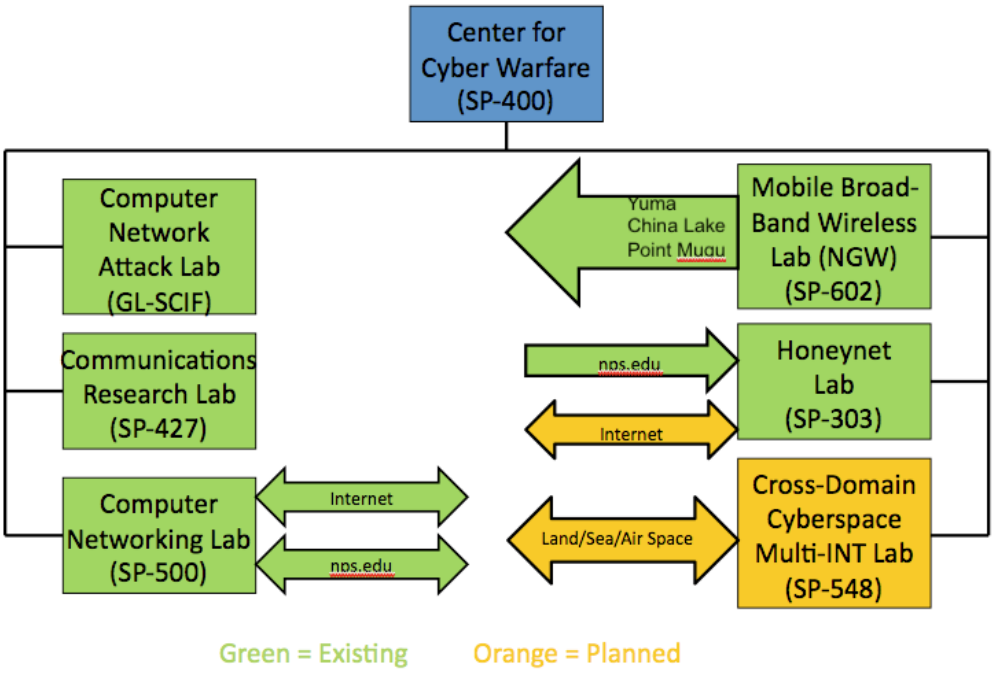

Figure 13. Center for Cyber Warfare Laboratories (From Knorr, 2010)

- **Computer Network Attack Laboratory**—this is one of three enablers of computer network operations (CNO), the laboratory is located in secure spaces and encompasses operations that disrupt, deny, degrade, and/or destroy information resident in computers and computer networks, or the computers/networks themselves.
- **Communications Research Laboratory**—the ECE department does a significant amount of research in the cryptology and other communications-related subjects under the aegis of the Center for Cryptologic Research. This laboratory provides hardware and software support of these projects.
- **Computer Networking Laboratory**—the laboratory supports instruction and research in the area of network design, engineering, and infrastructure development. Thesis work and research undertaken include modeling and simulation of high-speed and wireless networks and related protocols, video transmission over Asynchronous Transfer Mode (ATM) networks, traffic modeling, simulation and analysis, design and simulation of wide area networks, and related areas. Lab facilities include ATM switches, routers, Local Area Network (LAN) switches, video processing equipment, a channel simulator, a protocol analyzer, network simulation packages, and Windows New Technology (NT) workstations. The lab serves MSEE/EE degrees in both Communications and Computer tracks.

- **Honeynet Laboratory**—this laboratory incorporates Honeypot resources to detect, research, and prevent unauthorized or malicious access to network systems. The Honeynet Laboratory will allow students and researchers to develop a penetration, collection, and testing infrastructure focused on scanning the target environment external to the NPS domain, client and server side exploitation and post-exploit analysis of infected machines and arriving at potential resolutions. Acquired knowledge can be written as a Proof of Concept code to address exploitation techniques.
- **Mobile Broadband Wireless Laboratory**—research on LTE and WiMAX and future Institute of Electrical and Electronics Engineers (IEEE) 802 technologies will be focused in this laboratory.
- **Cross-Domain Cyberspace Laboratory**—functionally this laboratory will support in multi-INT disciplines. The primary collaborative partner will be NRO. (NPS ECE, 2010)

G. ENDSTATE

Figure 14 illustrates the desired end state for the CCW. The intent is to have CCW function as the premiere Academic Research Center of Excellence incorporating the key tenets of information dominance—Multi-Intelligence, Information Warfare, Information Technology, Space, Cyber Warfare while sustaining open collaboration with the government and private sectors across multiple classification levels through cross-domain technology. To accomplish this would require both buy-in from all key stakeholders depicted in Figure 14 and a proactive Community of Interest (COI) that follows a synergistic approach in the pursuit of emergent science and technology research initiatives.

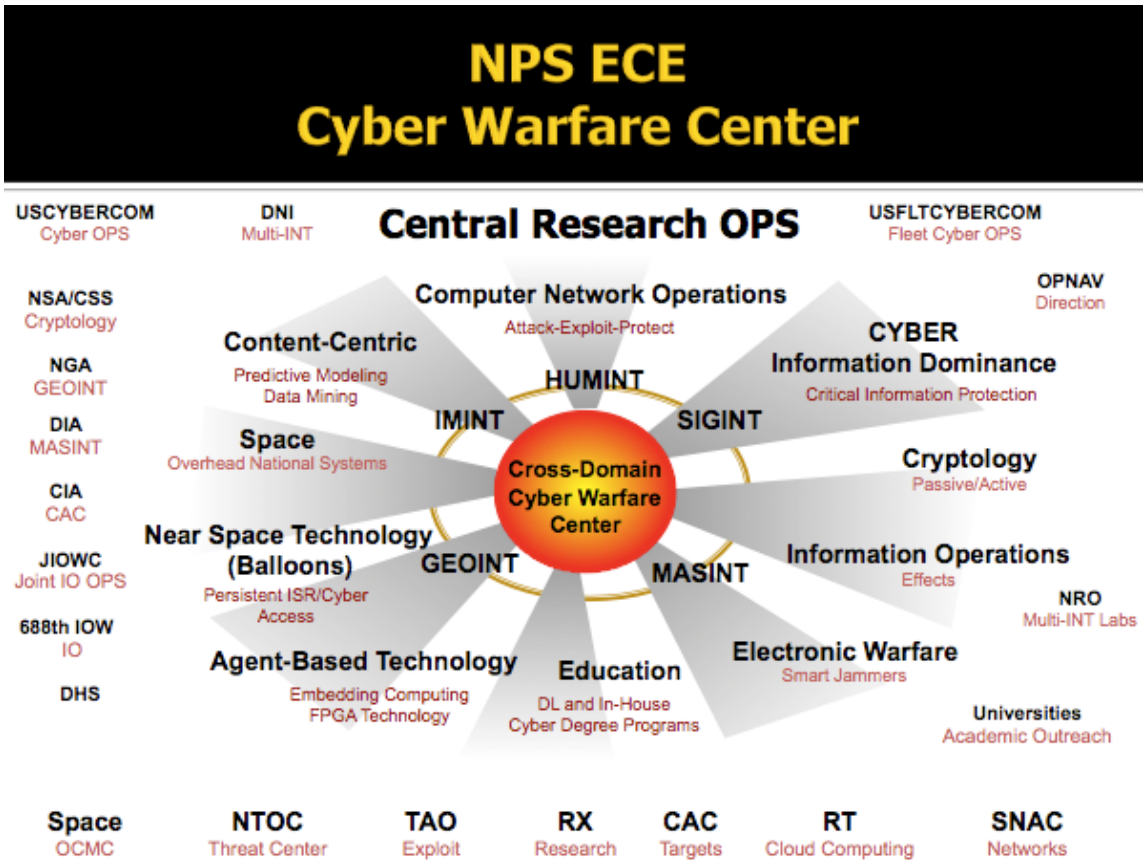

Figure 14. Future Cross-Domain Cyber Missions (From Garcia, 2010)

III. PROPOSED CCW NETWORK REQUIREMENTS

A. OVERVIEW OF DATA COMMUNICATION

Probabilities of analysis such as those studies conducted by Shannon that addressed the efficiency of communication channels in data transmissions played a decisive factor in utilizing the basic telephone network to initially transmit digital data. Figure 15 presents the fundamental building blocks of the communication model. The key elements are:

- **Source**—a device such as a workstation client that generates data for transmission.
- **Transmitter**—a medium that converts and programs information into a usable form for transmission across the wired/wireless network. For example, this could be a modem that takes 1s and 0s and converts it into an analog signal for delivery to a telephone network.
- **Transmission system**—a simple transmission line or complex network that routes and provides a connection between the source and destination.
- **Receiver**—a medium such as a modem or transmission line that senses incoming traffic and converts the received signal to a usable format for delivery to a destination device.
- **Destination**—end stage (i.e., server) that receives incoming data from receiver (Stallings, 1997).

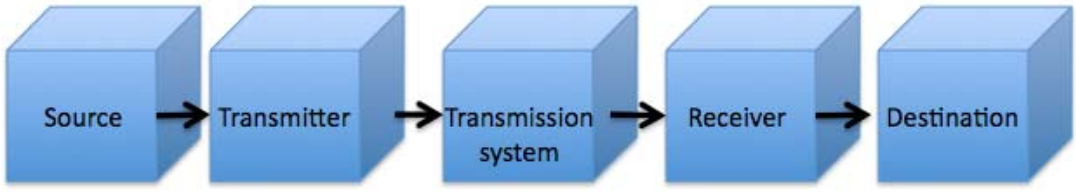

Figure 15. Simplified Communications Model (From Stallings, 1997)

The variables noted in Figure 15 enabled the exchange of information between two parties, a sender and a receiver via circuit switching technology such as the plain old telephone system (POTS). Today, while the basic telephone circuit continues to be employed in a communication network, more cost efficient means of both analog and digital transmission have evolved to solve the issues of distance between the source and destination and the need for a more robust system that can handle multiple transmissions at the same time. While packet switching technology opened the doors for multiple source clients to transmit data over a shared medium, a set of interoperable communication standards known as the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite followed suit and has formed the basis for what we know as the Internet.

B. CYBER INFRASTRUCTURE

Certain research and academic experimentation, testing, and evaluation although unclassified in nature will require deployment in a contained environment separate from the NPS campus network also referred to as the intranet. The CCW infrastructure will include a closed or private network, its associated network applications and network programming, data and network security, and Internet accessibility via a public network. CCW will additionally manage a detached server facility that consists of multiple operating systems and applications, a database repository for data storage and effortless retrieval of required resources, and internal backup system capabilities.

C. NETWORK REQUIREMENTS

Proper planning focused on architectural evaluation, prioritization, allocation of available resources and a thorough understanding of system requirements is crucial to the successful deployment of the chosen IT infrastructure. Currently, industry and military agencies are shifting away from stove-piped systems to a service oriented architecture (SOA) framework. Employment of an SOA environment delivers benefits in terms of the ability to leverage legacy systems, cost-efficiency, agility, adaptability, and

interoperability across multiple systems. To this end, again Figure 13 provides a block diagram of CCW laboratories that will need to be considered in the overall construct.

Software and system requirements needed to generate a fully operational IT infrastructure tend to be infinite in scope. In that respect, a fundamental provision prior to acquisition and deployment of systems is to draft a requirements document. At the outset, having a transparent layout of the scope of the project that may include areas such as requirements, assumptions, architecture, network protocols, networking hardware, topologies and access methods, etc. provides assurance that all key stakeholders have some understanding of the proposed architecture end state, reduces the risk of "mission creep" and additionally provides a chronological history of steps taken that can be referenced should they require it.

The network design should include a spreadsheet that lists all the devices that will have access to the network and addresses port and server requirements. Additionally, capacity planning that pertains to future growth should be factored in using the 15 percent rule. Another requirement that engineers typically overlooked that should be considered is the need for inter-switch trunks for firewall services or content service modules that typically have dedicated trunks. After identifying the number of ports needed, the next step would be to map out the port allocation and determine what devices will serve what purpose. These devices can then be further broken down to identify specific hardware requirements. In addition to port layouts, Internet protocol (IP) network and virtual local area network (VLAN) should be documented for future network configuration and reconfiguration. Also for consideration in Figure 16 is a bay face layout or diagram that provides a detailed illustration of the makeup of the rack that includes power, cabling, and patch panels requirements as well. Developing this layout offers that additional sanity check to ensure the server room can accommodate enough racks to support equipment purchased. Lastly, power in terms of alternating current/direct current (AC/DC), voltage, and amperage and cooling requirements should also be considered (Donahue, 2007).

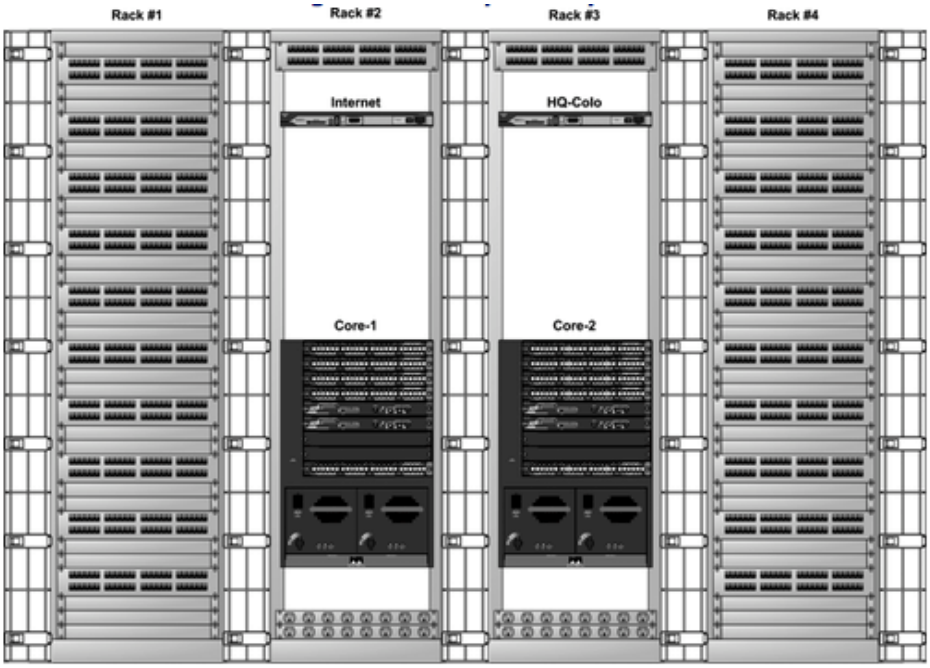

Figure 16. Bay Face Layout (From Donahue, 2007)

It must be noted that the above stated network requirements although it is not all-inclusive it does provide the key system requirements for the deployment of the CCW IT infrastructure. Additionally, while most network designs follow the classic three-tier model namely the core, distribution, and access levels, this CONOP document proposes the deployment of a virtual environment. Appendix A, added as an addendum addresses this virtual environment and discusses the framework, configuration, and equipment requirements for the proposed Honeynet Laboratory.

IV. CONCLUSIONS

Albert Einstein once said:

> The significant problem we face cannot be solved at the same level of thinking we were at when we created them.

And more recently, former DNI Mike McConnell made the statement as well that:

> If the nation went to war today, in a cyber war we would lose.

The urgency of developing a cadre of professionals trained to operate and conduct full spectrum operations in the cyber domain cannot be stressed enough. Malicious activity and attacks on network systems are here to stay for the interim or until scientists, engineers, academia, and military alike find a plausible solution to this issue. While other countries such as China, India, and Russia have official cyber warfare doctrines, development of U.S. doctrine that communicates our offensive and defensive cyber posture will likely be slow in coming (Gray, 2009, p. 217–219). Such is the case because our policy advisors need to deliberate and truly understand the ramifications our potential actions will have both at the national level and towards the international community as well. Moreover, while the concept of a well balanced strategy whether it be preemptive akin to the Cold War era or preventive with the intent to strike first to deter future aggressor actions seemingly appears to be the right option to pursue, the dynamic environment we live in restrains us from tying ourselves down to any one specific doctrine. In order to effectively operate in the cyberspace environment and maintain that competitive advantage over the adversary we need to build an agile cyber workforce strengthened by the collaborative partnerships between government agencies, the private sector, and academia. It requires a workforce with a predictive vice reactive mindset.

History elucidates the significance an academia-military alliance brings to the table and this serves as the cornerstone for CCW's philosophy on how to handle the emerging cyber threat. In 1941, the Office of Scientific Research and Development (OSRD) was established by then President Franklin D. Roosevelt for the purposes of

advancing military technology. This approach taken came with the realization that something had to be done right then and there to the best of OSRD capabilities and with the recognition that following this course of action came with the likelihood of potential failure. President Roosevelt was considered a very astute individual and using the academia-military partnership as a means to bring together a "mind meld" of both scientific and strategic intellect, he did achieve the desired end state of revolutionizing military capabilities through the development of weapons systems as illustrated in notable works such as the Manhattan Project from which the first atomic bombs evolved; sonar, radar to include technologies to defeat them known as electronic countermeasures (ECM), torpedo and amphibious vehicles; and sponsorship of Intelligence, Reconnaissance, and Surveillance (ISR) technology (Potente, 2010).

Current President of the United States (POTUS) Barak Obama is well aware of the numerous challenges that exist in cyberspace and his support of such is mirrored in recently promulgated documents on securing cyberspace and the formal implementation of a cybersecurity coordinator within the White House. In line with President Obama's actions, Secretary of Defense (SECDEF) Robert Gates subsequently passed a memorandum to the Joint Chiefs of Staff for the formal establishment of DoD entities focused on building capabilities to achieve information dominance in the air, land, sea, and space, all of which overlap in the cyber domain. In his words Secretary Gates made it transparent that:

> …modernization goals should be tied to the actual and prospective capabilities of known adversaries—not by what might be technologically feasible for a potential adversary given unlimited time and resources.

The foundation for the establishment of the cyber commands is based on the Phantom Fleet concept utilized during World War II, with four key variables given consideration—(1) the rank of the Commander to ensure his voice is heard and decisions made prevails; (2) shore establishment with capacity to commandeer operational units as the situation dictates; (3) small organization with access to all agencies without going through red tape; and (4) assumption of fleet status to maintain operational functionalities (Farago, 1962, p. 165). Additionally, to elicit full spectrum cyber operations the

Information Dominance Corps was formally established in January 2010 bringing together the disciplines of intelligence, information warfare, information technology, meteorology and oceanography, and the addition of cyber warfare. Such action has brought our information dominance strength to 45,000 personnel. From an academic standpoint, NPS CCW fits the bill to deliver the technical foundation for the potential cyber workforce who will support requirements and fill the operational billets of these organizations similar to the OSRD academia-military alliance in 1941…"but how so?" one may ask.

Consider the terms – data, information, and knowledge. While there is some truth in that all three are dynamically interrelated, people do tend to use them interchangeably forgetting that each variable performs a very distinct process. To better understand this relationship—data is typically associated with 1s and 0s. Data, in its raw form, is useless to the average person (with the exception of those individuals who have inherent tacit knowledge of what those 1s and 0s actually mean). In taking this data one can analyze it further or convert it into some usable form referred to here as information. Exposure to such data and information then generates knowledge that an individual can use to make more informed decisions if not only to enhance his explicit knowledge. Explicit or "codified" knowledge in this case refers to knowledge that is transmittable in formal, systematic language whereas tacit knowledge is personal, context-specific, and therefore hard to formalize and communicate (Nonaka & Takeuchi, 1995).

The key takeaway here is that to acquire this knowledge requires some form of learning. As suggested earlier, CCW has ECE faculty and research staff that has the background and expertise to influence growth and reinforce the explicit knowledge base of its students through education and cutting-edge research. History dictates that learning through action and knowing through motion does breed distinction (Nissen, 2006). Over the last century, NPS has managed to deliver prominence in the battlefield in the likes of ADM Arleigh Burke a graduate of Chemical Engineering, ADM James Watkins in Mechanical Engineering, GEN Michael Hagee in Electrical Engineering and more recently, ADM Michael Mullen earning distinction in the field of Operations Research

and GEN Alexander in the fields of EW and Physics. Again, to gain information dominance requires creation and sustainment of such knowledge through learning.

This thesis prescribes a concept of operations document and framework that can serve as the baseline for further work and refinement. As presented in the preceding chapters, this thesis proposes an operational construct wherein buy-in from key stakeholders within the disciplines of intelligence, information warfare, information technology, space, meteorology and oceanography, and cyber warfare is essential. As VADM McCullough FLTCYBERCOM/C10F Commander stated:

> One of our lines of operation (LOO) is to achieve and sustain the ability to navigate and maneuver freely in cyberspace and the RF spectrum.

By interconnecting the above stated disciplines, the capability to achieve information dominance across cyberspace becomes more apparent (McCullough, 2010).

Emergent technology calls for adoption of a more adaptive and agile cyber infrastructure and we propose such with the conjectural framework illustrated in Chapter III. As illustrated in Appendix A, successful deployment of a Honeynet within other academic institutions and results derived from employment of research initiatives similar to the Honeynet Project shows potential where CCW researchers and students have access to real time raw data that they can analyze and draw from.

In closing, CCW exhibits strong potential to emerge as a premier facility to train the next generation cyber workforce. Tie this in together with the robust collaborative network current ECE faculty and associate researchers have built with existing government agencies and universities and CCW is well on its way to conducting full spectrum cyberspace education and research operations that reaches across all domains and leverages CCW ability to emerge as the primary Academic Research Center of Excellence - Cyberspace. Investing in cutting edge research and development is not a want but a must and from this research and parallel cyber education, the acquisition and deployment of emergent technology will help sustain future battles in the cyber domain (Deputy Assistant Secretary of the Navy, 2010).

V. RECOMMENDATIONS

Recommendations for future work would be to align CCW's highly technical graduate program with written governing laws and policies. While not covered in detail, a book released by the National Academies Press (NAP) titled "Technology, Policy, Law and Ethics Regarding U.S. Acquisition and use of Cyberattack Capabilities" provides fundamental insight on courses of action and moral principles to consider with regards to the acquisition and proper use of cyber attack capabilities. Further research on these issues of legal and ethics rights; policy; technical and operational capabilities; and organizational structure will facilitate and provide focus on future CCW research and development initiatives as well as prepare undergraduates with the requisite skill sets to analyze cyber networks and recognize characteristics that requires employment of offensive and defensive cyber actions (Owens, Dam & Lin, 2009). Defining the rules of engagement (ROE) particularly with respect to—(1) the chain of command structure for notification of initiation of attacks, (2) when to execute an attack, (3) who can be targeted, (4) duration of cyber activities, and (5) conditions for exception to ROE are just a few issues for consideration (Carr, 2009).

Further exploration on the correlation between the standard cyber attack methodology referenced in Chapter I and the U.S. phases of operation needs to be analyzed. Phase 0 Shaping and Phase I operations pertain to the deployment of resources to collection background information in order to gain situational awareness of the current environment. Similar to Phase II operations, scanning pertains to exploitation of known vulnerabilities or holes in the system. As is in Phase III operations, the attacker dominates by gaining access to systems either through illegitimate means or known weaknesses in network systems. In Phase IV, the attacker is attempting to stabilize his operating environment through data deletion, theft, alteration, and storing of malware. In Phase V, the attacker now has access to the infected system and has the ability to enable and redeploy malware at will.

Initiate additional investigation of other technologies currently being fielded that exhibits the potential for application towards research of cyber initiatives currently underway at NPS. For example, Figure 17 depicts a network management tool that provides a graphical user interface (GUI) of current cyber situation. Indicators and lists provide near real time threat condition and defensive posture of network systems.

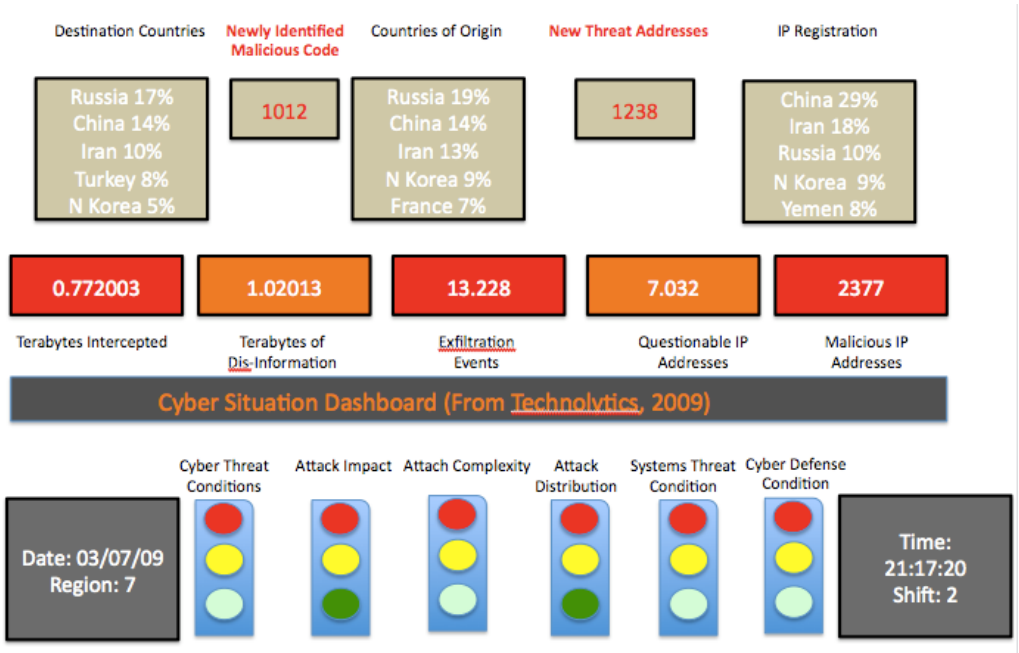

Figure 17. Cyber Situation Dashboard (From Technolytics, 2009)

Commence development of a more comprehensive definition of hardware and software requirements to support a fully functional Cyber Warfare Research Center. The architecture and server hardware equipment listing proposed in Appendix A was based on information obtained from applicable documents and a study of existing virtual Honeynet installations. Appendix A covered the essential features needed to deploy a virtual server but there are a myriad of options that still need to be considered in determining the feasibility of this virtual environment. A more practical follow on to this thesis is to incorporate the remaining five research areas and provide a more thorough discussion of other existing or emerging technology. Again due consideration should also be given to ensure that the deployed network environment will be flexible and agile enough to handle future mission set requirements without having to sacrifice cost and/or efficiency.

APPENDIX HONEYNET PROJECT

At the writing of this thesis, ECE determined that the Honeynet Laboratory would be the primary focus for the initial architectural construct. A robust, scalable network with an analogous configuration that can later be implemented to support additional research and education initiatives such as cross-domain transfer technology, computer network attack, computer network operations, mobile broadband wireless, and communications research was also considered to ensure rapid implementation of the aforementioned services. This section discusses a viable data communication network comprised of interconnected nodes and links that supports deployment of multiple operating system platforms and applications and allows for pooling of available resources to increase operational efficiency.

A. HONEYNET OVERVIEW

Honeypots are the resources and methodologies utilized to detect, research, and prevent unauthorized or malicious access to network systems. A Honeynet on the other hand is a type of Honeypot primarily used for research.

Research on the evolution of "Honeypots" that being, methodologies used to gather data and information for analysis on attacks and compromise of workstations confirms that numerous systems and techniques exist. The Deception Toolkit (DTK) developed by Fred Cohen, one of the pioneers in developing a system that gave the appearance of network vulnerabilities; Cybercop Sting developed by Network Associates, Inc. that was built as a decoy server; Netfacade from Verizon; BackOfficer Friendly (BOF) focused primarily on Back Orifice attacks; Specter supported by Netsec; Honeyd a prepackaged open source Unix honeypot; and Symantec's Mantrap also known as Decoy Server are all examples of commercially available honeypots.

The Honeynet, in this case was selected for several reasons. First, the Honeynet can emulate multiple commercially available operating systems vice focusing solely on a single system. Second, as suggested earlier, it is an effective research tool because as a

high interaction Honeypot it allows the attacker to interact with an actual operating system. Third, a global consortium known as the "Honeynet Project" exists that is committed to providing shared situational awareness of the current extant threats that exist in network systems and additionally provides the necessary tools and innovative techniques to deter cyber threats. Fourth, one can learn from studies completed by the different factions and also derive proven techniques to increase efficiency in the initial installation and setup of the CCW laboratory. Lastly, the NPS ECE faculty has had exposure to the Honeynet environment in the past thereby reducing potential downtime of having to educate and train the staff prior to the deployment of the Honeynet Laboratory.

With this in mind, the intent of this section then is to offer an adaptive approach focused on the establishment of a small-scale testing and server environment; in this case a virtual Honeynet environment.

B. HONEYNET FRAMEWORK

It has been established that the operating environment would incorporate both physical and virtual infrastructure therefore the task of migration of current infrastructure was determined as having minimal impact to the overall construct of the proposed framework. Not withstanding, to ensure seamless transition key players such as network administrators, developers, security administrators, IT management, storage administrators, and operating system administrators must all be brought onboard and understand the unique and new concepts that virtualization provides.

It has also been determined that a service-oriented architecture (SOA) framework should be implemented vice stove-piped system architecture. An SOA framework will ensure interoperability of the multiple operating systems and associated languages, allow use of standard, commercial off the shelf (COTS) technology vice proprietary systems, and ability to reuse components thus increasing efficiency while decreasing overall costs. In line with this the key stakeholders must ensure that requirements both functional and non-functional are clearly delineated prior to implementation. While the initial installation will be for the Honeynet Laboratory, requirements should address other

research initiatives as well to ensure acquisition of appropriate server and equipment and to account for load balancing; electrical; heating, ventilating, and air conditioning (HVAC); and space requirements.

One must also note that there is inherent risk associated with running a Honeynet Laboratory and use of this specific Honeypot configuration requires strict adherence to best business practices and system rules. To mitigate these risks, standard operating procedures (SOP) should address and follow policies set by Information Technology and Communications Services (ITACS) and Department of the Navy Chief Information Officer (DONCIO) in concert with the universal practice of employing firewalls, Intrusion Detection Systems (IDS), segregation of testing environment from network, and virtual private network (VPN) as deemed applicable. A report generated by Joseph Greenfield identified that the laboratory be comprised of three elements—a closed, secure network environment for malware analysis; an open network for Honeynet analysis; and a hybrid configuration to support classroom instruction and experimentation with computer security countermeasures (Greenfield, 2010).

C. HONEYNET LABORATORY REQUIREMENTS

The standard virtualization hypervisors out on the market are Citrix Xenserver and VMware vSphere. Based on research of existing software and technology, a virtualized environment utilizing VMware infrastructure was preferred for several reasons. VMware allows for multiple operating systems to be deployed on the same physical medium. Physical hardware can be configured or partitioned for more efficient use of available resources. Studies have shown the Honeynet architecture being deployed in analogous academic environments and how it has yielded valuable data results that can be used for further analysis of cyber attacks patterns. Additionally, VMware's robust, scalable platform permits for deployment in supplementary initiatives such as with cross-domain transfer that has already gained NSA approval.

While VMware offers different versions of Elastic Sky X (ESX) this thesis covers deployment of such utilizing the Enterprise edition. Consideration was given based on several key requirements:

- Need for a network that can support thousands of systems.
- Service console allows for command line operations and running script.
- Allocates space for additional components.
- Compatibility with different vendor models.
- Centralized Virtual Machine (VM) management.
- Built in firewall that protects service console.
- Supports booting for a storage area network (SAN) providing quick recovery time for affected VM (Siebert, 2009, p. 29–30).

In determining server hardware requirements VMware offers a Capacity Planner toolkit for business partners intending to purchase VM applicable services. In lieu of this, Tables 3 through 5 provides estimations based on the set rules derived from the VMware implementation guide (Siebert, 2009, p. 48–65).

- The number of required host servers is defined by CPU and memory requirements.
- CPU activity determines number of VMs allocated per ESX host. Rule of thumb – single core supports four single-vCPU VMs.
- Advanced memory feature in ESX reduces amount of physical host memory utilized prevents added performance degradation.
- Hard disk usage should be based on the amount used excluding free space.
- ESX currently supports Intel and Broadcom network interface card (NIC). Consider four-port adapter for greater flexibility and reliability.
- iSCSI as a network storage is the preferred cheaper alternative.
- Network attached storage (NAS) provides an additional fault network storage option comparable to iSCSI.
- VMware Vsphere 4.0 allows for complete deployment versus individual server management (Troy & Halmke, 2010, p. 3).
- Redundant Array of Independent (or Inexpensive) Disks (RAID) supports fault tolerance for shared data and applications. RAID 1 utilized for disk mirroring or data backup. RAID 5 incorporates distributed parity with disk striping (Dean, 2006, p. 689–693).
- Storage Area Networks (SANs) are storage devices that support direct communication between entities (Dean, 2006, p. 694–696).

More specific guidelines can be found in a report released by Joseph Greenfield, August 31, 2010.

Manufacturer	Dell
Model	PowerEdge R710
Size	2U Bracket for Xeon 56xx Processor and 8 2.5” hard drives
CPU	(2) Intel Xeon E5620 2.4GHz, 12M Cache, Turbo, HT, 1066MHz max memory
Memory (RAM)	(8x8GB) 64GB memory, 1333MHz dual ranked RDIMMs for 2 processors, optimized, advanced ECC
Primary Hard Disks (OS)	(2) 72GB 15K RPM SAS Hot Plug Hard Drive, RAID 1
Secondary Hard Disks (Virtual Machines)	(6) 500GB 7.2K RPM SAS 2.5” Hot Plug Hard Drive, RAID 5
Power Supply	High Output 870W Redundant Power Supply
Network Adapters	(2) Onboard GB Ethernet NIC, Broadcom 5709 Dual Port 1GB Ethernet NIC with TOE PCIe-4
Additional NIC	(2) Broadcom 5709 Dual Port 1 GB Ethernet NIC

Table 3. Virtualization Server Specifications (From Greenfield, 2010)

Manufacturer	Dell
Model	R210
Size	1U
CPU	Intel Xeon X3440, 2.53GHz, 8M Cache, Turbo, HT
Memory (RAM)	(4x2GB) 8GB memory, 1333MHz, Dual Ranked UDIMM
Hard Disks	(2) 600GB 15K RPM Serial-Attached SCSI 6Gbps 2.5” Hot Plug, RAID 1
Network Adapters	(2) Onboard GB Ethernet NIC, Broadcom 5709 Dual Port 1GB Ethernet NIC with TOE PCIe-4
Optical Drive	SATA DVD-ROM

Table 4. Control Server Specifications (From Greenfield, 2010)

Rack Hardware	32U Server Rack
	(3) 3U Uninterruptible Power Supplies
	2U Managed Switch
	1U Control Server
	(10) 2U Virtualization Server
Additional Hardware	8TB Netgear Ready NAS
Software	MSDNAA Developers
	VMware vSphere 4

Table 5. Honeynet Hardware Requirements (From Greenfield, 2010)

D. HONEYNET CONFIGURATION

Figure 18 illustrates the proposed logical topology for the CCW laboratory. Here logical topology references the data transmission methodology between nodes. In a bus topology, signal travels from one network device to all other network devices whereas in a ring topology signals follow a circular path between the sender and receiver.

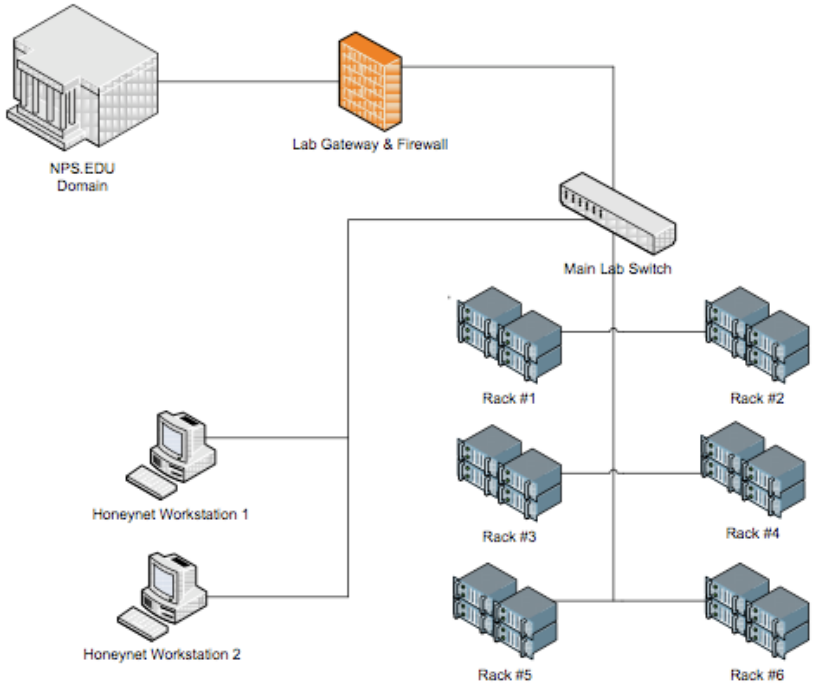

Figure 18. Proposed Logical Network Topology (From Greenfield, 2010)

Figure 19 depicts a typical Honeynet comprised of a Host Operating System (OS) such as Linux or Windows and three separate network interfaces. Implementation of the Honeynet is accomplished using VMware, a commercially available software program. A bridge interface is used to connect the different network segments for two reasons. Bridges are protocol independent therefore data transfers a more rapid rate. Bridges also have a database to filter out unwanted frames that in turn improves overall system performance.

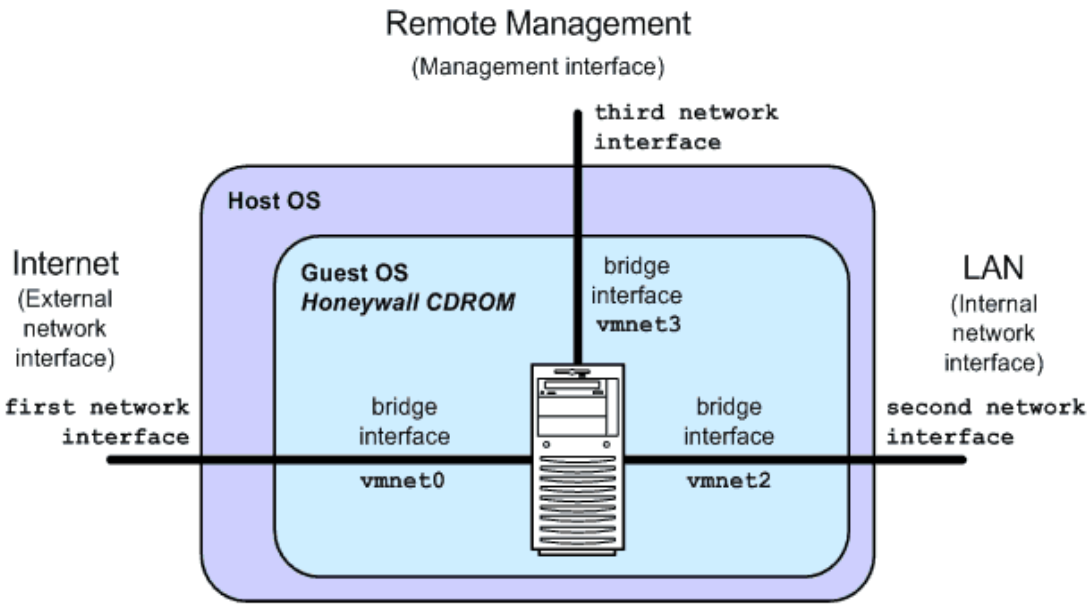

Figure 19. General Architecture (From Honeynet Project, 2004)

Figure 20 further goes on to illustrate a Honeynet uploaded with the Honeywall compact disc read only memory (CDROM) comprised of both virtual and real Honeypots. It shows the Honeynet environment enclosed in a detached environment that when in bridge mode has the capability to emulate a legitimate network system running application and services that are accessible to a potential hacker. The hacker or attacker in this case is any individual that utilizes either opportunistic or targeted approach to exploit vulnerabilities in a system. Opportunistic attacks in this case are incidents in which an attacker has a general idea of what or whom he wants to attack. Targeted attacks on the other hand are attacks in which the attacker specifically chooses his target and does not give up until his target is compromised (Dhajani, Rios, & Hardin, 2009, p. 223–224).

Based on the construct, the attacker would have the ability to hack into the hybrid Honeynet and unbeknownst to the hacker, it gives the administrator access to methodologies used by the hacker to enter into the isolated network system. A key point to be made is that this entire evolution can transpire without having to worry about the security risks or potential compromise of the entire system.

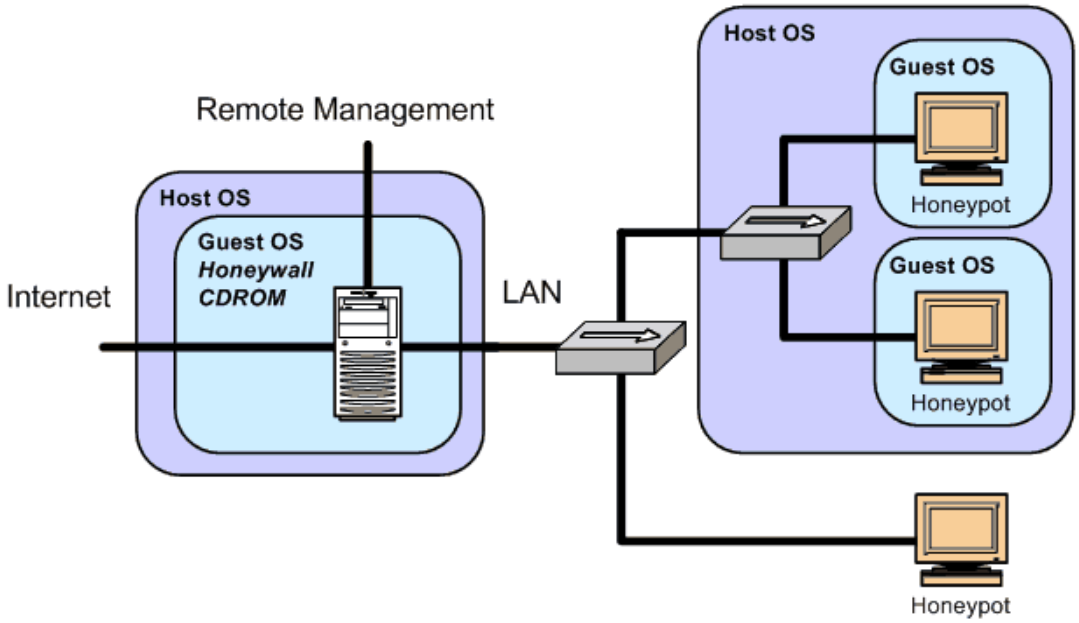

Figure 20. Hybrid Virtual Honeynet (From Honeynet Project, November 2004)

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Azarov, S., & Dodonov, A. (2006). *Instrumental corrections for a definition of Cyberwar*. Amsterdam, Netherlands: IOS Press.

Beltz, N. (1999). *Cryptologic research laboratory* document. Monterey, California: Naval Postgraduate School.

Bothamley, J. (2002). *Dictionary of theories.* Canton, Michigan: Visible Ink Press.

Braun, R. (2010). Information dominance corps. Brief circulated by RDML Robin Braun, Director N2N6C1 Total Force Management.

Bush, G. W. (2008). Homeland Security Presidential Directive 23. *Cybersecurity and monitoring.* Washington, D.C.: White House. Retrieved on March 15, 2010, from http://www.fas.org/irp/offdocs/nspd/index.html

Bush, G. W. (2008). *House Permanent Select Committee on Intelligence white paper on cyber security*. Washington, D.C.: White House. Retrieved on March 15, 2010, from http://www.whitehouse.gov/files/documents/cyber/Congress%20-%20HPSCI%20White%20Paper%20on%20Cyber--Final%20DEC%2008.pdf

Bush, G. W. (2008). National Security Presidential Directive 16. *Guidelines for offensive cyber warfare*. Washington, D.C.: White House. Retrieved on March 15, 2010, from http://www.fas.org/irp/offdocs/nspd/index.html

Carr, J. (2009). *Inside cyber warfare.* Sebastopol, California: O'Reilly Media Incorporated.

Carvalho, F. (2006). *CyberWar-Netwar: Security in the information ag*e. Fairfax, Virginia: IOS Press.

Cebrowski Institute for Information Dominance Web portal. (2010). Retrieved on January 22, 2010, from http://www.nps.edu/cebrowski/index.html

Center for Strategic and International Studies. (2008). *Securing cyberspace for the 44th presidency*. Washington, D.C.: Center for Strategic and International Studies. Available from http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

Central Intelligence Agency. (2010). "*Mission Statement.*" Retrieved on January 22, 2010, from https://www.cia.gov/about-cia/cia-vision-mission-values/index.html

Chief of Naval Operations. (2010). OPNAV Instruction *The Corps of information communities.* Washington, D.C.: OPNAV, 2010.

Clarke, R. & Knake, R. (2010). *Cyber war: The next threat to national security and what to do about it.* New York, New York: HarperCollins Publishers.

Commander, U.S. Tenth Fleet. (2010). *"Mission Statement."* Information Dominance Corps manual.

Commander, U.S. Tenth Fleet. (2010). C10F task organization chart. Washington, D.C.

Computer History. (2010). Retrieved on January 15, 2010, from http://www.computerhistory.org/Internet_history/

Cyberspace. *Merriam-Webster's Online Dictionary*. (2010). Retrieved on January 22, 2010, from http://www.merriam-webster.com/dictionary/cyberspace

Dean, T. (2006). *Network+ guide to networks*. Boston, Massachusetts: Thompson Course Technology.

Defense Intelligence Agency. (2010). *"Mission Statement."* Retrieved on January 22, 2010, from http://diajobs.dia.mil/DIAintro.html

Defense Technical Information Center. (2010). *Information dominance and the U.S. Navy's cyber warfare vision.* Retrieved on April 30, 2010, from http://www.dtic.mil/ndia/2010SET/Dorsett.pdf

Defense Technical Information Center. (2010). Joint Publication 1-02. *Joint operations planning.* Retrieved on August 21, 2010, from http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf

Defense Technical Information Center. (2010). Joint Publication 5-0. *Department of Defense dictionary of military and associated terms. "Cyberspace."* Retrieved on August 21, 2010, from http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Delbert, R. & Rohozinski, R. (2009). *Tracking GhostNet: A cyber espionage.* Retrieved on August 18, 2010, from http://www.tracking-ghost.net

Department of Defense Directive 5000. (2008). *Defense acquisition system.* Washington, D.C.: DoD. Retrieved on September 9, 2010, from http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf

Department of Defense Directive 5100.20. (2010). National Security Agency/Central Security Service "*Mission Statement."* Washington, D.C.: DoD. Retrieved on September 9, 2010, from http://www.dtic.mil/whs/directives/corres/pdf/510020p.pdf

Department of Defense. (2003). *The national strategy to secure cyberspace.* Washington, D.C.: White House. Retrieved on September 8, 2010, from http://www.dhs.gov/files/publications/publication_0016.shtm

Department of Defense. (2006). Chairman, U.S. Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations "Definition of cyberspace operations."* Washington, D.C.: CJCS. Retrieved on January 22, 2010, from http://www.dod.mil/pubs/foi/ojcs/072105doc1.pdf

Department of Defense. (2010). *Annual report to Congress: military and security developments involving the People's Republic of China.* Washington, D.C.: DoD. Retrieved on September 6, 2010, from http://www.defense.gov/pubs/pdfs/2010_CMPR_Final.pdf

Department of Defense. (2010). *Quadrennial defense review report 2010.* Washington, D.C.: SECDEF. Retrieved on March 10, 2010, from http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf

Department of Homeland Security. (2008). *Information technology security essential body of knowledge: A competency and functional framework for IT security workforce development.* Washington, D.C.: DHS.

Department of Homeland Security. (2010). *"Mission Statement."* Retrieved on January 22, 2010, from http://www.dhs.gov/xlibrary/assets/DHS_StratPlan_FINAL_spread.pdf

Department of the Navy. (2009). SECNAVINST 3052.2. *Cyberspace policy and administration within the Department of the Navy.* Washington, D.C.: Secretary of the Navy. Available from http://doni.daps.dla.mil/Directives/03000%20Naval%20Operations%20and%20Readiness/03-00%20General%20Operations%20and%20Readiness%20Support/3052.2.pdf

Deputy Assistant Secretary of the Navy. (2010). *What does a cyber secure Navy look like? Cyber protection, prioritization, and plan.* Brief circulated by Brian Shaw, DASN C4I / IO / Space.

Dhajani, N., Rios, B., & Hardin, B. (2009). *Hacking: the next generation.* Sebastopol, California: O'Reilly Media Incorporated.

Director of National Intelligence. (2010). *"Mission Statement."* Retrieved on January 22, 2010, from http://www.dni.gov/

Donahue, G. (2007). *Network warrior.* Sebastopol, California: O'Reilly Media Incorporated.

Dorsett, J. (2009). Email Message for the Information Dominance Corps. *Information Dominance Initiatives*.

Farago, L. (1962). *The Tenth Fleet.* New York, New York: Ivan Obolensky Incorporated.

Federal Communications Commission. (2010). *"Mission Statement."* Retrieved on September 13, 2010, from http://www.fcc.gov/

Filipowski, S. (2010). *Navy information dominance industry day.* Brief circulated by RDML Sean Filipowski, Director N2N6F3 Cyber, Sensors and Electronic Warfare.

Fleet Cyber Command (FLTCYBERCOM). (2010). *"Mission Statement."* Retrieved on April 30, 2010, from http://www.fcc.navy.mil/

Garcia, V. (2010). *Future cross-domain cyber missions.* Monterey, California: NPS.

Gorman S. (2009). "Electricity grid in U.S. penetrated by spies," *Wall Street Journal*. April 8, 2009, Retrieved on September 2, 2010, from http://online.wsj.com/article/SB123914805204099085.html

Gray, C. (2009). *National security dilemmas: Challenges and opportunities.* Dulles, Virginia: Potomac Books, Incorporated.

Greenfield, J. (2010). *Honeynet project.* Report prepared for NPS Department of Electrical and Computer Engineering. Monterey, California: NPS.

Higgins. K. (2010). '*Aurora'attacks still under way, investigators closing in on malware creators*. Retrieved on September 8, 2010, from http://www.darkreading.com/vulnerability_management/security/attacks/showArticle.jhtml?articleID=222700786

Honeynet Project. (2010). *"Know your enemy: Defining virtual honeynet."* Retrieved on August 21, 2010, from http://old.honeynet.org/papers/virtual/

Information Professional. (2010). Community training symposium brief presented 25 January 2010.

Institute of Electrical and Electronics Engineers. (2010). *"Mission Statement."* Retrieved on September 13, 2010, from http://www.ieee.org/about/vision_mission.html

International Telecommunication Union. (2010). *"Mission Statement."* Retrieved on September 13, 2010, from http://www.itu.int/net/about/mission.aspx

Internet World Statistics. (2010). Retrieved on September 1, 2010, from http://www.Internetworldstats.com/stats.htm

Ketchen, D., Snow, C., & Hoover, V. (2004). Research on competitive dynamics: Recent accomplishments and future challenges. *Journal of Management*, 30, 779-884. http://jom.sagepub.com/content/30/6/779.full.pdf+html

Knorr, J. (2009). *NPS cyber research and education for the IDC: Recommendations for action to align NPS research and graduate education with current Navy vision.* Monterey, California: NPS.

Knorr, J. (2010). *Framework for a cyber roadmap*. Prepared for OPNAV Information Dominance. Monterey, California: Naval Postgraduate School.

Knorr, J. (2010). *MS in Cyber Space and Operations matrix*. Prepared for Department of Homeland Security. Monterey, California: Naval Postgraduate School.

Maravedis. (2010). *WiMax and LTE deployment map*. Retrieved on September 10, 2010, from https://www1.vtrenz.net/imarkownerfiles/ownerassets/328/4GCounts_Operator_Deployment_Map.pdf

Markoff, J. (2009). "Vast spy system loots computers in 103 countries" *New York Times*, March 28, 2009. Retrieved on January 25, 2010, from http://www.nytimes.com/2009/03/29/technology/29spy.html

McCullough, B. (2010). *Way Ahead for FLTCYBERCOM/C10F*. Brief provided by VADM Bernard McCullough to the Information Dominance Corps.

McEachen, J. (2009). *Threat level orange: How much can you count on your wireless mobile device?* Brief circulated to academia and industry October 29, 2009. http://www.nps.edu/Academics/Institutes/Cebrowski/News-and-Events/cybersummit/docs/McEachenCyberSummitreleasable.pdf

National Geospatial-Intelligence Agency (NGA). (2010). "*Mission Statement.*" Retrieved on January 22, 2010, from http://www.dni.gov/overview.pdf

National Reconnaissance Office (NRO). (2010). "*Mission Profile.*" Retrieved on January 22, 2010, from http://www.dni.gov/overview.pdf

National Science Foundation (NSF). (2010). "*Mission Statement.*" Retrieved on January 22, 2010, from http://www.nsf.gov/about/glance.jsp

Naval Education and Training (NAVEDTRA) 43360. (2010). *Information Dominance Corps personnel qualification standards - preliminary draft.* Pensacola, Florida: Naval Education and Training Command.

Naval Education and Training (NAVEDTRA) M-130B. (2009). *Task based curriculum development manual volume III manager's guide.* Pensacola, Florida: Naval Education and Training Command.

Naval Postgraduate School *Information Technology Strategic Plan.* (2009). Monterey, California: Naval Postgraduate School.

Naval Postgraduate School Instruction (NAVPGSCOLINST) 3900.2. (1999). *Establishment and operation of research centers of excellence at Naval Postgraduate School.* Monterey, California: Naval Postgraduate School. Retrieved on January 25, 2010, from http://intranet.nps.edu/code00/Instructions/pdf_files/NPSINST%203900.2A.PDF

Naval Postgraduate School. (2010). "*Mission Statement.*" Secretary of the Navy Instruction 1524.2A dated April 4, 1989. Retrieved on January 25, 2010, from http://intranet.nps.edu

Naval Postgraduate School. Electrical and Computer Engineering Department Web portal. Retrieved on January 25, 2010, from http://www.nps.edu/Academics/Schools/GSEAS/Departments/ECE/

Nissen, M. (2006). *Harnessing knowledge dynamics: Principled organizational knowing & learning.* Hershey, Pennsylvania: IRM Press.

Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company*. New York, New York: Oxford University Press.

Obama, B. (2010). *Comprehensive national cybersecurity initiative*. Washington D.C.: White House, 2010. Retrieved on March 15, 2010, from http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

Owens, W., Dam K., & Lin, H. (2009). *Technology, policy, law and ethics regarding U.S. acquisition and use of cyberattack capabilities.* Washington, D.C.: National Academies Press. Available from http://www.nap.edu/catalog.php?record_id=12651

Potente, G. (2010). *Developing a cyber workforce: A Navy cyber challenge.* Brief circulated by CAPT Gene Potente, OPNAV Information Dominance.

Prasad, R. & Kim, Y. (2006). *4G roadmap and emerging communication technologies.* Norwood, Massachusetts: Artech House.

Siebert, E. (2009). *VMware implementation and administration.* Boston, Massachusetts: Prentice Hall.

Stallings, W. (1997). *Data and computer communications.* Saddle River, New Jersey: Prentice Hall.

Technolytics Institute. (2009). *Cyber commander's handbook.* McMurray, Pennsylvania: Technolytics Institute.

Thompson, M. (1995). "Onward Cyber Soldiers" *Time Magazine*. Retrieved on September 2, 2010, from http://www.time.com/time/printout/0,8816,983318,00.html

Troy, R. & Helmke, M. (2009). *VMware cookbook.* Sebastopol, California: O'Reilly Media Incorporated.

United States Cyber Command (USCYBERCOM). (2010). *"Mission Statement."* Retrieved on January 22, 2010, from http://www.stratcom.mil/factsheets/cc/

United States Naval Academy (USNA) Cyber Warfare Center. (2010). *"Mission Statement."* Retrieved on March 15, 2010, from http://www.usna.edu/cyber/

United States Navy. (2010). *Chief of Naval Operations Guidance for 2010.* Executing the maritime strategy. Washington, D.C.: CNO, 2009. Retrieved on August 1, 2010, from http://www.navy.mil/features/CNOG%202010.pdf

United States Tenth Fleet (10th Fleet). (2010). *"Mission Statement."* Retrieved on April 17, 2010, from http://www.fcc.navy.mil/

Van Houten, V. (2010). *An Overview of the Cyber Warfare, Exploitation & Information Dominance (CWEID) Lab.* Retrieved on September 15, 2010, from http://info.publicintelligence.net/cyberwarfarebrief.pdf

Wentz, L., Barry C., & Starr, S. (2009). *Military perspectives of cyberpower.* Washington, D.C.: National Defense University.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dean, Graduate School of Engineering and Applied Sciences
   Naval Postgraduate School
   Monterey, California

4. Chair, Information Sciences Department
   Naval Postgraduate School
   Monterey, California

5. Intelligence Chair
   ADM Andrew Singer, Ret. USN
   Naval Postgraduate School
   Monterey, California

6. Director, Center for Cyber Warfare
   Naval Postgraduate School
   Monterey, California

7. CAPT Daniel Burns, USN
   Naval Postgraduate School
   Monterey, California

8. CAPT Vicente Garcia, Ret. USN
   Naval Postgraduate School
   Monterey, California

9. Senior Intelligence Officer
   CAPT Jennith Hoyt, USN
   Naval Postgraduate School
   Monterey, California

10. CAPT Douglas Small
    Program Executive Office
    Integrated Warfare Systems 2

11. Professor Tri Ha
Naval Postgraduate School
Monterey, California

12. CDR John Van Hise, Ret. USN
Naval Postgraduate School
Monterey, California

13. Christopher Parente
PMW120 IO PAPM
San Diego, California

14. Rita Painter
SPAWARSYSCEN Pacific
CODE 56130 IO/ISR