2016-03

Fighting the network: MANET management in support of littoral operations

Maupin, Matthew S.

Monterey, California: Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

FIGHTING THE NETWORK: MANET MANAGEMENT IN SUPPORT OF LITTORAL OPERATIONS

by

Matthew S. Maupin

March 2016

Thesis Advisor: Alex Bordetsky
Second Reader: Wayne Porter

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			*Form Approved OMB No. 0704–0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2016	**3. REPORT TYPE AND DATES COVERED** Master's thesis	
4. TITLE AND SUBTITLE FIGHTING THE NETWORK: MANET MANAGEMENT IN SUPPORT OF LITTORAL OPERATIONS			**5. FUNDING NUMBERS**
6. AUTHOR(S) Matthew S. Maupin			
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)

Advances in computer processing and communications capabilities have contributed to the recent explosion of mesh network technologies. These technologies' operational benefits are of particular interest for those operating in the littorals. The dynamic complexities of the littorals force tactical decision-makers to adapt to a constantly changing battlespace in a constrained temporal and spatial environment. Ongoing research into the integration of unmanned systems and sensors as mobile ad-hoc network (MANET) nodes highlights the significant potential to improve situational awareness and force efficiency in the littoral environment. However, difficulties associated with tactical network operations and management make the littorals particularly challenging. There remains a need for a unified approach to managing these networks in a coherent and effective manner. The complexity of the littorals emphasizes the inherent interconnectedness of MANET management and command and control (C2). As a result, new and innovative approaches to C2 are also required. This thesis explores the value of modern network management systems as they contribute to the richness of the human-network interface, as well as the integration of network management and maneuver at the tactical level. The result is a proposal for a novel framework for littoral MANET management and C2 as a corollary of cyber-physical maneuver.

14. SUBJECT TERMS mesh networking, MANET, command and control, littoral operations			**15. NUMBER OF PAGES** 111
			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

FIGHTING THE NETWORK: MANET MANAGEMENT IN SUPPORT OF LITTORAL OPERATIONS

Matthew S. Maupin
Lieutenant, United States Navy
B.S., Oregon State University, 2009

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN NETWORK OPERATIONS AND TECHNOLOGY

from the

NAVAL POSTGRADUATE SCHOOL
March 2016

Approved by: Alex Bordetsky
Thesis Advisor

Wayne Porter
Second Reader

Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Advances in computer processing and communications capabilities have contributed to the recent explosion of mesh network technologies. These technologies' operational benefits are of particular interest for those operating in the littorals. The dynamic complexities of the littorals force tactical decision-makers to adapt to a constantly changing battlespace in a constrained temporal and spatial environment. Ongoing research into the integration of unmanned systems and sensors as mobile ad-hoc network (MANET) nodes highlights the significant potential to improve situational awareness and force efficiency in the littoral environment. However, difficulties associated with tactical network operations and management make the littorals particularly challenging. There remains a need for a unified approach to managing these networks in a coherent and effective manner. The complexity of the littorals emphasizes the inherent interconnectedness of MANET management and command and control (C2). As a result, new and innovative approaches to C2 are also required. This thesis explores the value of modern network management systems as they contribute to the richness of the human-network interface, as well as the integration of network management and maneuver at the tactical level. The result is a proposal for a novel framework for littoral MANET management and C2 as a corollary of cyber-physical maneuver.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

A2/AD	Anti-Access/Area Denial
AO	Area of Operations
AFP	Adaptive Force Package
API	Application Program Interface
ARAM	Adaptable Radiation Area Monitor
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CHOMP	Configure, Heal, Optimize, Monitor, Protect
CONOPS	Concept of Operations
CoT	Cursor on Target
CPS	Cyber-Physical Systems
CPSS	Cyber-Physical-Social Systems
DSS	Decision Support System
DL	Distributed Lethality
DLTF	Distributed Lethality Task Force
EMIO	Expanded Maritime Interception Operations
EPF	Expeditionary Fast Transport
ESB	Expeditionary Mobile Base
FCAPS	Fault, Configuration, Accounting, Performance, Security
FIAC	Fast Inshore Attack Craft
HCI	Human-Computer Interface
ICS	Internet Connection Sharing
ISO	International Standards Organization
JFC	Joint Force Commander
JOA	Joint Operations Area
KML	Keyhole Markup Language
LCS	Littoral Combat Ship
LOC	Littoral Operations Center
LLNL	Lawrence Livermore National Laboratories
MANET	Mobile Ad-hoc Network

MIB	Management Information Base
MRT	Media Richness Theory
NCW	Network Centric Warfare
NMIOTC	North Atlantic Treaty Organization Maritime Interdiction Operations Training Center
NMS	Network Management System
NSO	Network Service Orchestrator
NWDSS	Network Decision Support System
NOC	Network Operations Center
OODA	Observe, Orient, Decide, Act
OTAR	Over-the-Air Rekey
OTAZ	Over-the-Air Zeroize
PLI	Position Location Information
PPDIO	Prepare, Plan, Design, Implement, Operate, Optimize
ROV	Remotely Operated Vehicle
SA	Situational Awareness
SAG	Surface Action Group
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
STK	Systems Tool Kit
TMN	Telecommunications Management Network
UAV	Unmanned Aerial Vehicle
UGV	Unmanned Ground Vehicle
UUV	Unmanned Underwater Vehicle
VOI	Vessel of Interest
VPN	Virtual Private Network
VBSS	Visit, Board, Search and Seizure
WMN	Wireless Mesh Network

ACKNOWLEDGMENTS

Many individuals contributed to this research and supported me along the way. I owe an enormous debt of gratitude to Dr. Alex Bordetsky for advising me on this thesis and opening my mind to a completely new understanding of “outside-the-box” thinking. When I first asked Dr. Wayne Porter to be my second reader, I had no idea what a tremendous impact he would have on my work and on me personally—I cannot thank him enough for guiding me through this process. Similarly, Steve Mullins was there for me every step of the way; he is truly the bond that keeps CENETIX together. Of course, I have to thank my roommate and friend, Tim Kirkpatrick, for keeping the lights on for me after the long days in the lab. Finally, for Eugene Bourakov, Malcolm Mejia, and the CENETIX student research team—Adam Sinsel, Rob Schultz, Mike Pothitos, and others—I am especially grateful for their insights and friendship throughout this endeavor.

Above all, I express my sincere gratitude to my beloved wife, Kathryn, for standing by me as I embarked upon the journey of completing my Master of Science. Without her love and support, none of this would have ever been possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Littoral waters will be the arena of modern fleet action.
—W. P. Hughes (2000, p. 165)

CAPT Wayne P. Hughes (USN, ret.) (2000) describes the littorals as a complex and dynamic operating domain characterized by dense commercial and maritime traffic, diverse terrain features, and a chaotic RF environment. Difficulties associated with tactical network operations and management make the littorals particularly challenging for naval forces. However, the performance characteristics of mesh networking technologies make them particularly well suited to address some of these shortfalls.[1] The attributes of mesh networks—including the ability to dynamically self-organize, integrate with existing infrastructure, and provide reliable fault-tolerant connectivity across a highly scalable coverage area—make them an attractive solution for use in a multitude of applications (Misra, Misra, & Woungang, 2009). Haider and Shabbir (2014) assert that a mesh approach is "the right solution to enable highly mobile, highly reactive and quickly deployable maritime tactical networks" (p. 488).

The U.S. Naval Surface Warfare community's recent shift toward "distributed lethality" provides a prime example of the potential tactical advantages that maritime tactical mesh networks could provide, particularly in the littorals. Distributed Lethality (DL) is a maturing concept under development by the Distributed Lethality Task Force (DLTF). This concept is described by VADM Rowden, RADM Gumataotao, and RDML Fanta (2015) as "the condition gained by increasing the offensive power of individual components of the surface force." Expanding the capacity of the surface fleet for executing offensive operations is the goal of DL (Solomon, 2015). DL widens the scope of naval Surface Action Groups (SAG) operations, introducing the concept of Adaptive Force Package (AFP) operations that integrate traditional and non-traditional platforms to provide "agile, tailorable combatant forces." These evolving and adaptive force structures

[1] It is important to note that the use of the term "mesh network" in this thesis refers primarily to Mobile Ad-Hoc Networks (MANET) as opposed to Wireless Mesh Networks (WMN); this multi-hop networking nuance is explicated in Chapter II.

seem to demand a robust mesh network to ensure effective command and control (C2) during sea control operations constrained or contested littoral environments.

Current academic maritime mesh network research focuses primarily on commercial applications for archipelagic nations or countries with high-density maritime traffic. Research into the application of mesh technologies to military maritime tactical networks has received relatively minimal academic consideration; there is even less research concerning the management of these networks. Regardless, the Department of Defense is moving forward with the development, testing and evaluation of advanced multi-hop tactical networking systems. The integration of these systems into military operations will require novel approaches to C2. The new generation of network management systems (NMS) surpasses the quality of existing tools and enables network operators to function beyond contemporary network management paradigms.

Distributed mesh network operations in the littorals require new and innovative approaches to command and control. Bordetsky and Netzer (2010) introduce the concept of adaptive management patterns as a function of mesh node positioning (mobility management) and application load control. Subsequently, Bordetsky, Benson and Hughes (2015) offer the concept of cyber-physical maneuver as the manifestation of adaptive management, as applied to littoral operations. New management tools can realize cyber-physical maneuver by enabling network operators to influence the tactical placement of various platforms, thus allowing decision-makers to consider the location of physical assets and resource allocation as a function of mission requirements and application load.

Increasing the richness of the human-network interface through the graphic display of network performance information is intended to help tactical-level decision makers process and adapt to changes in the battlespace more effectively. This requires a fundamental shift in how network management is operationalized. This thesis demonstrates that viewing a unified network management system as an integrated element of C2, as opposed to a support function, can ultimately aid the self-synchronization of small-scale groups of heterogeneous assets operating in complex tactical environments.

A. LITTORAL OPERATIONS

Ambiguity regarding the definition of the term "littoral" continues to spark debate across military and academic circles. Though the Merriam-Webster dictionary definition of this word is suitable for general use—"of, relating to, or situated or growing on or near a shore especially of the sea"—it is not always fully comprehended or clearly defined in its application (Vego, 2015). Joint Publication 1-02 (Joint Chiefs of Staff, 2015a) bifurcates the definition into two parts—"Seaward: the area from the open ocean to the shore, which must be controlled to support operations ashore," and "Landward: the area inland from the shore that can be supported and defended directly from the sea" (p. 146). This explanation adds some clarity to the wordlist definition but lacks overall precision and fails to account for all pertinent geographical circumstances (Vego, 2015). Vego (2015) explains that the littorals "encompass areas bordering the waters of open peripheral seas, large archipelagoes, and enclosed and semienclosed seas" (p. 33). The addition of Vego's geographic description provides perspective regarding the constituent areas of the littoral domain.

The Naval Postgraduate School's Littoral Operations Center (LOC) seeks to further the Navy's ongoing efforts to expand its knowledge in this arena. The center's mission is to conduct interdisciplinary research supporting U.S. Navy, allied and partner nation policy, strategy and technology development in support of littoral operations. The LOC (Naval Postgraduate School, n.d.) describes the littorals more broadly as the area where "hydrography, geography, commerce, fishing, mining, boundaries, maneuver and sustainment issues converge and complicate both the Offense and the Defense, to place exceptional demands on naval, aerial, and land forces that must operate, fight, and influence events there." The convergence of these notions in the congested and contested coastal waters and their adjacent terrain illustrates the importance of continued study of this multi-faceted problem space.

Difficulties faced in the littoral environment are especially evident across several hotbeds of tension, such as the Baltic and South China Seas, where the U.S. Navy and its allies face ever-growing challenges to power projection. Additionally, the increasing sophistication of anti-access/area denial (A2/AD) strategies and threat proliferation

continue to threaten the U.S Navy's ability to operate freely in the maritime commons (Department of the Navy, 2015). Forces deployed in A2/AD environments face potential degradation of timely and relevant knowledge of the operating environment and disrupted or degraded C2 mechanisms. The inherent complexity of the littorals compounds the difficulties associated with operating in A2/AD environments, particularly when it is recognized that access denial will likely include cyber networks and the electromagnetic spectrum upon which operations so heavily depend. Bypassing littoral waters by projecting power ashore from a distance may work temporarily, however, operations will eventually require naval forces to operate in the littorals (Wade, 1996). In order to create and maintain sea control in this contested littoral environment, forces need to understand the battlespace and its impact on their ability to integrate forces and aggregate their collective effects.

In "A Cooperative Strategy for 21st Century Seapower" (Department of the Navy, 2015), Secretary Mabus outlines the concept of cross-domain synergy for the Joint Force to overcome the challenges posed by the A2/AD threat. The elements Secretary Mabus lists are particularly challenging in the littorals. However, mesh networks provide an opportunity to enhance joint force capabilities in this environment, especially considering these factors:

- Battlespace awareness—networked assets can provide leadership with a more complete and timely understanding of the environment in which forces are operating.
- Assured command and control—mesh networks provide self-forming, self-healing networks can provide flexible, robust, and resilient networks that will gracefully degrade in contested environments.
- Cyberspace operations—network-centric capabilities embodied in mesh networks will enhance power projection capabilities for operations in cyberspace and their cyber-physical impacts.
- Electromagnetic maneuver warfare—the hybrid nature of the network architectures discussed in this thesis support the future integration of alternative networking concepts such as those proposed in the Network Optional Warfare concept in development at NPS. Additionally, leveraging the heterogeneity of network assets through the development of EMCON and MILDEC tactics can enhance the impact of these networks.

- Integrated fires—the ability to create temporary areas of battlespace control supported by the flexibility and scalability of mesh networks expands the Joint Force Commander's kinetic and non-kinetic options in contested environments.

While this list explicates the significance of mesh network concepts through a strategic/operational lens, this thesis focuses on their implementation and management at the tactical level.

B. LITTORAL OPERATIONS SCENARIO

The benefits of emerging MANET and Network Management technology can enhance force capabilities across the range of military operations; however, the CENETIX Counter-Weapons of Mass Destruction (CWMD) and Maritime Interception Operations (MIO) experiments provide unique opportunities to explore the application of new network management systems. Chapter III discusses the details of these experiments. MIO is defined as "efforts to monitor, query, and board merchant vessels in international waters to enforce sanctions against other nations such as those in support of United Nations Security Council Resolutions and/or prevent the transport of restricted goods" (Joint Chiefs of Staff, 2015a, p. 150). JP 1-02 delineates CWMD as "efforts against actors of concern to curtail the conceptualization, development, possession, proliferation, use, and effects of weapons of mass destruction, related expertise, materials, technologies, and means of delivery" (Joint Chiefs of Staff, 2015a, p. 53). Expanded Maritime Interception Operations (EMIO) are an extension of MIO that refers to the interception of vessels transporting terrorist-related materiel that pose an imminent threat and other related missions authorized by the President to prevent attacks against the United States (Joint Chiefs of Staff, 2011). The scenario framework used for the experiment provides relevant context with which to analyze potential concepts of operations (CONOPS) and how these systems can influence tactical operations in the littorals. Consider the following scenario:

Naval forces are tasked to conduct EMIO in support of ongoing CWMD operations in a contested littoral region. An AFP consisting of three Littoral Combat Ships (LCS) is operating in the area and has received intelligence that an unmarked small

fast inshore attack craft (FIAC) recently embarked a container of shielded nuclear material and/or residue that was previously GPS-tagged by special operations forces in an earlier sensitive site exploitation (SSE) operation. The LCS Maritime Operations Center (MOC) receives information that this FIAC is operating in an area of dense maritime traffic near a busy commercial port. Equipped with modified-SUW mission packages, the LCS deploy several SeaFox USVs equipped with optical and standoff radiological/nuclear detection devices. Several BlackJack UAVs with optical sensors are also launched to conduct an area search for the vessel of interest (VOI). In addition to organic unmanned assets, several Mark VI patrol boats are under the tactical control of the AFP Commander and are equipped to conduct Visit, Board, Search and Seizure operations. All assets are equipped with MANET systems. Adversaries in the region are known to have shore-based mobile communications jamming capabilities.

This vignette provides a contemporary and germane milieu for prospective missions and challenges faced by littoral forces. It is used as a framework to demonstrate the flexibility and resiliency MANETs can provide if C2 processes adapt to support them.

C. RESEARCH OBJECTIVES

U.S. littoral or blue-water forces do not yet have a standardized self-organizing, self-healing mobile ad-hoc network across the full spectrum of operations… but the building blocks are in place (K. Rothenhaus, personal communication, 15 January 2016). The purpose of this research is to explore solutions that can effectively leverage scalable and flexible communication infrastructures within the littoral operating environment to provide the tactical advantage. The primary question addressed in this research is the following:

> How can emerging network management tools support tactical-level mesh networks and influence C2 in littoral operations?

Pursuing the answer to this question will address corollary objectives that include exploring the unique capabilities network operators need to support these operations and what opportunities non-traditional platforms can provide in littoral mesh-networked operations.

D. SCOPE AND LIMITATIONS

This research question explores mesh network operations to support new changes in C2, tactical maneuver, and the integration of dispersed naval forces operating in the littoral domain. It focuses on the application of network management software to the maneuver of ship nodes at the tactical level and investigates the potential and impact of these systems to provide network awareness to tactical-level decision makers.

Discussion along the way inquires into network management capabilities required to monitor and manage dynamic mesh network performance in the littoral environment and looks to identify new networking roles for traditional and non-traditional platforms (e.g., using ships, such as LCS or off-shore basing platforms, and unmanned systems as foundational elements). This discussion examines the feasibility of integrating network management technologies into operations to strengthen littoral C4ISR capabilities and explores a littoral mesh network concept of operations for operating in conjunction with manned, unmanned and/or shore-based assets.

This thesis does not address the operational or strategic level implications of mesh networks; rather it focuses on their tactical implementation in a littoral maritime environment. This work is done through experimental scenarios, not with fielded naval vessels, and does not address the technological deficiencies of currently fielded mesh networking technologies.

E. ORGANIZATION OF THESIS

Chapters II provides literature review of supporting research and concepts relevant to research objectives. Chapter III outlines the research design and simulation modeling conducted to support littoral mesh networking concepts. Chapter IV is an overview of the experimentation results and description of potential use cases, as well as a discussion of NMS feasibility and constraints. Chapter V summarizes the overall conclusions reached and outlines future work.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

The separation in traditional organizational structures between higher-level decision makers and lower-level elements controlling and monitoring decision implementation is a consequence of risk management (Fama & Jensen, 1983). However, in some cases, this separation may result in a functional disconnect between the operational decision maker and the network operator at the lowest tier; a decision maker may not even be aware of the physical network configuration supporting their operations. Likewise, a network operator may only be cognizant of the network for which they are responsible, yet unaware of factors that influence higher-level operational decisions. Changes in either domain are filtered within and through multiple organizational layers before adjustments are made. Effective network-enabled operations in the complex littorals require a minimization of that separation; a direct "connection" between decision makers and the physical network provided by network decision support tools is important for effective force deployment.

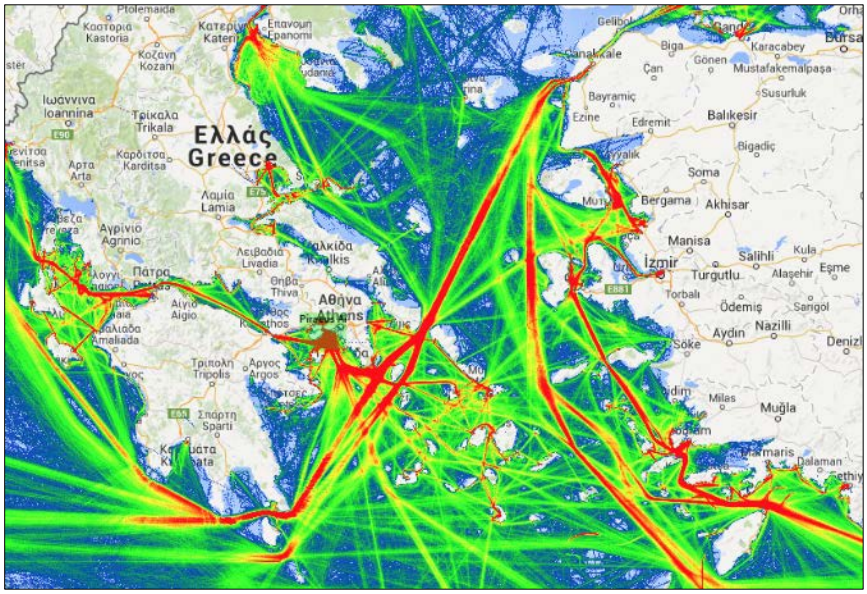
A. NETWORK OPERATIONS CHALLENGES

The Network Centric Warfare (NCW) concept proposes that the networking of assets to create a "well-informed but geographically dispersed force" will improve the efficiency and effectiveness of military operations (Cebrowski & Garstka, 1998, p. 8). Robust networks enhance information sharing and collaboration, creating shared situational awareness (SA) and self-synchronization (Alberts, 2002). By creating a network of reconnaissance, C2, and weapons systems; full spectrum dominance is achievable across the range of military operations (Koch & Golling, 2015). Cebrowski and Gartska (1998) also assert that the superiority provided by improved situational awareness of the environment, a better understanding of the operational situation, and the dramatic acceleration of decision-making cycles would allow the massing of effects from a lighter and leaner fighting force to disrupt the enemy's C2 processes.

1. Organizational and Technological Impacts of Littoral Complexity

Operations in the coastal and near-shore regions face considerably different conditions than those conducted in the open ocean. Complexity characterizes the physical characteristics of the littorals as well as the nature of the operations conducted there. One can define complexity as the interaction, interconnectivity and inter-relationship among elements of a system and between the system and its surroundings (Chan, 2001). Even in their most permissive state, operations in the littorals are constrained by interference factors from the surrounding environment. The land-sea interface that characterizes the littoral region brings with it the effects of diverse environmental conditions and dense commercial traffic. Figure 1 shows an example of shipping traffic concentrations in the littoral zone. It illustrates the conditions of physical clutter, which in turn create the preconditions for clutter in the cyber realm. Environmental conditions above and below the surface (e.g., sea state, fog, subsurface hazards and tidal patterns) present challenges for both offensive and defensive naval operations (Lindberg & Todd, 2001).

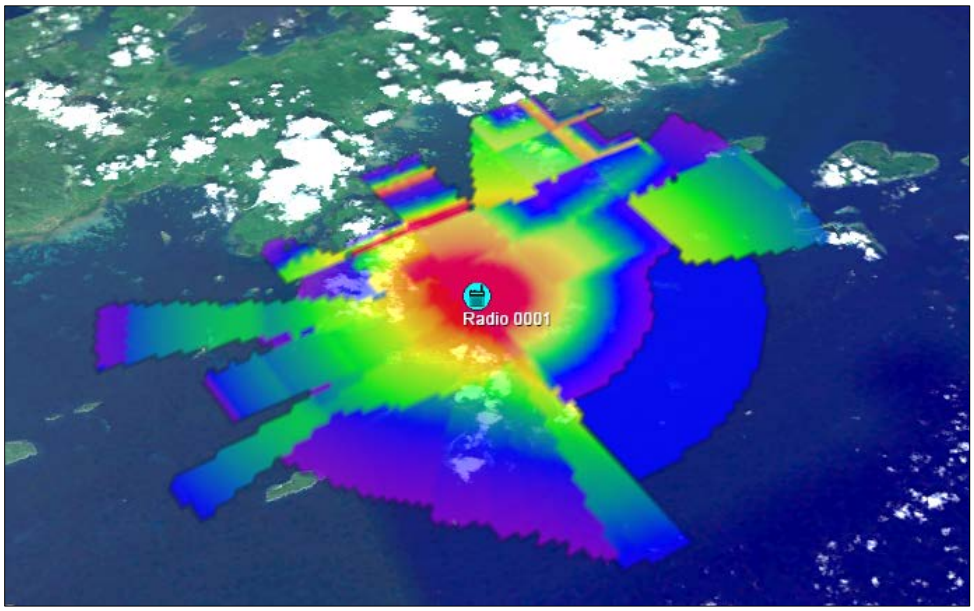
Figure 1. Shipping Traffic Density Map of the Aegean Sea



Source: Aegean Sea marine traffic: Marine vessel traffic. (n.d.). Retrieved January 14, 2016, from http://www.marinevesseltraffic.com/2013/06/aegean-sea-marine-traffic.html

Terrain is a major factor that differentiates blue water operations from those in the littorals. Topographical features such as cliffs, islands, vegetation, etc., not only impede on a maritime force's ability to maneuver, but also their ability to manipulate and control the RF spectrum. Geography and meteorological/oceanographic conditions can attenuate signals or completely inhibit the ability of ships to communicate with each other. Figure 2 illustrates the effect that terrain can have on maritime communications system propagation. These factors represent significant obstacles for communications networks, but at the same time offer additional opportunities for multi-hop relay networking.

Figure 2. Radio Coverage Analysis of Notional Communications System in Littoral Zone



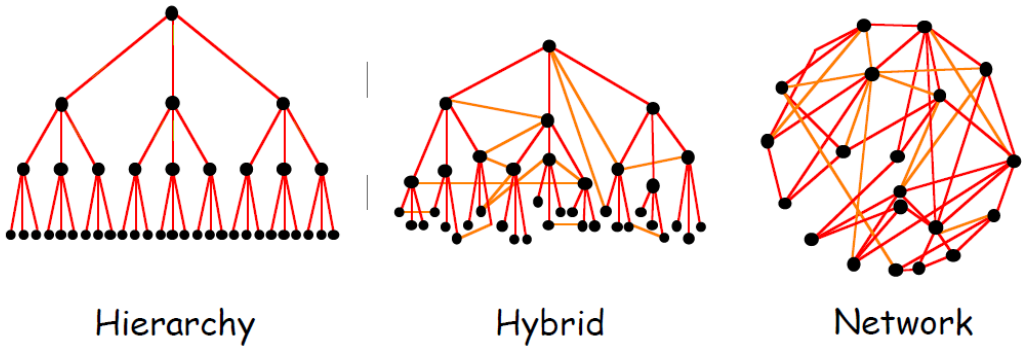
This radio coverage analysis shows signal-to-noise (SNR) levels as they interact with terrain features with red as the highest SNR and blue/violet as the regions with lowest SNR relative to the source.

Proximity to shore presents another set of problems for forces operating in the littorals. While distances might be measured in thousands of miles in the open ocean, the littorals provide defenders the ability to rapidly deploy surface and subsurface assets from shorter distances (Vego, 2015). Off-shore islands, archipelagos and other features can be used to obfuscate enemy forces or allow them to intermingle with neutral maritime traffic

(Lindberg & Todd, 2001). Additionally, littoral forces find themselves deep within the effective range of modern coastal defense systems (Ya'ari, 2014). These could include defense batteries as well as short-range attack and reconnaissance aircraft, enemy UAVs, or other systems. Rear Admiral Ya'ari, Israel Navy, (2014) asserts that "the short distances within the littoral arena create acute problems of reduced reaction time and 'threat bearing'" (p. 82). Naval forces must adapt to these conditions to dominate opposing forces in the littoral environment.

The complexity of operations is therefore influenced by enemy action (including those in the cyber realm), environmental interference, and the actions of the friendly force itself. From a C2 perspective, endogenous organizational complexity and the exogenous environment of operations should drive organizational and technological design; the complexity of force structure should match that which it faces. Bar-Yam's (2003) Multiscale Complex Systems Analysis of Littoral Warfare concludes that warfare cannot be effectively performed in the highly complex littorals without first addressing organizational and technological deficiencies—primarily the need for "radically different coordination mechanisms in high complexity environments" (p. 23). This leads to the recognition that traditional organizational hierarchies are less effective when dealing with coordination across elements of an organization to execute tasks of high complexity. Van Creveld (1985) points out that systems will naturally become more complex to enable the transmission of information vertically, as well as laterally, between subordinate units. This adaptation subsequently changes the organizational structure of the force itself. Bar-Yam (2003) offers the notion of "Form for Function," pointing out that littoral warfare necessitates fine scale representation, e.g., small independently acting groups, flatter organizational structures, and more distributed control. Figure 3 depicts various control structures.

Figure 3. Control Structure Examples of Varying Complexity



Source: Bar-Yam, Y. (2003). Complexity of military conflict: Multiscale complex systems analysis of littoral warfare. Cambridge, MA. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.132.6248&rep=rep1&type=pdf

The collaboration-enabled, self-organizing nature of small-unit groups at the tactical edge provides increased ability to sense, process and adapt to changes in the operating environment. In this case, complexity and adaptability complement each other. Adaptive systems are more likely to endure environmental disruptions and allow for smooth responses to changes in information conditions (Cares, 2005). However, reflecting this organizational adaptability in the technical networking methods used to connect them is critical.

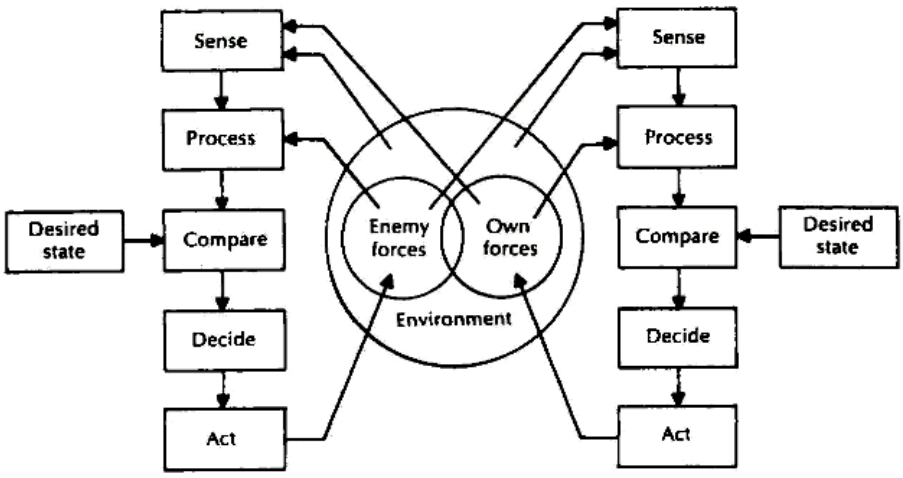
2. Impacts of Littoral Complexity on Decision-making Processes

In addition to driving organizational and technological requirements, the complex context of the littorals unavoidably influences a decision maker's perceptions, interpretations and actions within a decision space. Decisions in this domain must balance risk, uncertainty, and the additional constraints related to the presence of physical and cyber clutter unique to the littorals.

In his landmark book, *Command in War*, Van Creveld (1985) proposes that one way a C2 structure can compensate for uncertainty in combat is by increasing the processing capacity of its decision-making cycles. The Lawson Command-Control Cycle describes C2 processes as they influence, or are influenced by, their surrounding environment (Sweeney, 2002). Hughes (2000) takes the Lawson cycle a step further to rectify what he refers to as a "flagrant deficiency [that] treated control as a one-sided

process" (p. 214). He addresses this by expanding Lawson's cycle to illustrate the interaction between friendly and enemy C2 cycles across shared environment of clutter. Bordetsky, Benson and Hughes (2015) add that the opposing actions of anti-scouting, command and control counter-measures, and counterforce (countering the enemy's ability to sense, decide and act) are critical, network-dependent processes. The networking of sensors, shooters and decision-makers in a shared information ecosystem allows forces to discover and disrupt enemy activities more quickly and efficiently. Figure 4 shows Hughes' modified Lawson C2 cycle.

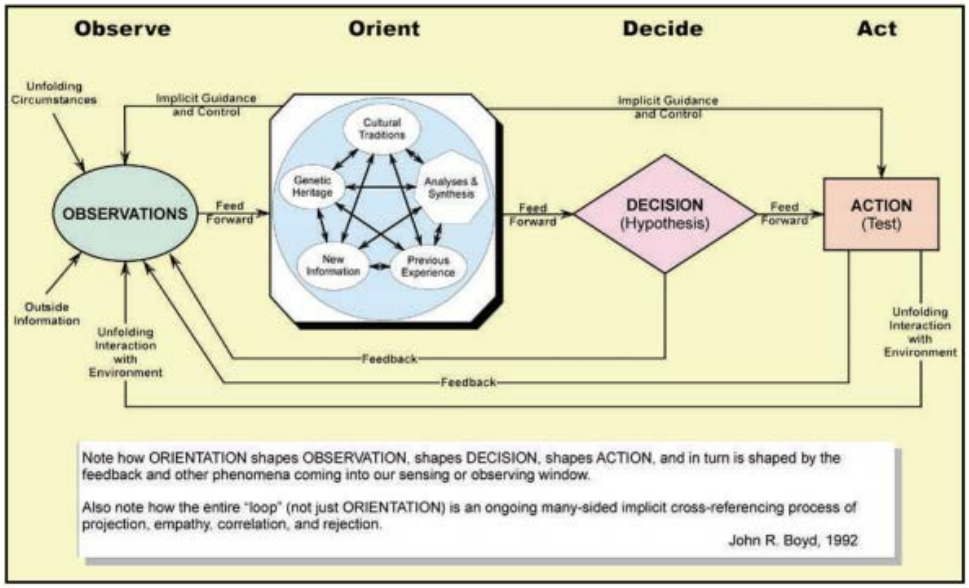
Figure 4. Hughes' Modified Lawson Command-Control Cycle



Source: Hughes, W. P. (2000). *Fleet tactics and coastal combat* (2nd ed.). Annapolis, MD: Naval Institute Press.

Another popular decision framework is the Observe-Orient-Decide-Act (OODA) loop, first introduced by John Boyd in 1987. Grant and Kooter (2005), discuss OODA and provide a comparison to other models in terms of C2 architectures. Boyd's OODA loop is depicted in Figure 5.

Figure 5. Boyd's OODA Loop



Source: Dettmer, H. W. (2011). *Systems thinking and the cynefin framework—A strategic approach to managing complex systems*. Port Angeles, WA: Goal Systems International.

It is important for decision makers to be cognizant of the context within which they are operating—the causal relationships that exist between different types of systems inform the implementation of these decision-making processes. Snowden and Boone's 2007 Harvard Business Review article introduces the Cynefin sense-making framework that identifies five contexts in terms of the relationship between cause and effect: simple, complicated, complex, chaotic, and disorder. The simple and complicated domains represent ordered systems in which there is a recognizable relationship between cause and effect, although it may not be readily apparent. Whereas, in the chaotic and complex domains, this relationship either does not exist or can only be perceived in retrospect. Disorder occurs "when it is unclear which of the other four contexts is predominant" (Snowden & Boone, n.d.). The boundaries between these areas represent transitions between decision domains; decision states move between these domains as the situation evolves. Snowden links the Cynefin framework to the OODA decision model by pointing out that "each domain needs its own variation of OODA" (Snowden, 2012). Figure 6 illustrates the Cynefin framework and the decision models appropriate for each domain.

Figure 6. The Cynefin Framework

Source: Cognitive Edge. (n.d.). The cynefin framework [video]. Retrieved February 23, 2016, from https://www.cognitive-edge.com

Interacting elements at all levels of decision making with the littorals produce nonlinear, dynamic systems that shift decisions in the littorals from the ordered decision domain and into the complex domain. There are no right answers to decisions in the complex domain because of the unknowable relationship between cause and effect (Snowden & Boone, n.d.; Snowden, 2012). As a result, patterns in emergent order instruct new or unique approaches to problems—what Snowden (n.d.) refers to as "emergent practice." Subsequently, the decision model offered by Snowden and Boone (n.d.) is probe-sense-respond.

Traditionally, Boyd's OODA loop is applied to situations in which it is assumed the tactical environment is stable enough to rapidly orient forces, decide, and act upon observable phenomena. An inference that might be drawn from the work of Snowden and Boone (n.d.) is that there are four decision domains only one of which, simple, and possibly a second, complicated, lend themselves to the traditional application of the OODA loop. What Lawson and Hughes are attempting to address is a reformulation of the command-control decision loop that is flexible enough to be effective in the other two decision domains, chaotic and complex. In littoral operations, interaction not only with

the environment but also with the adversary's own decision cycle represents a significant tactical challenge that should be considered in the context of a complex decision domain.

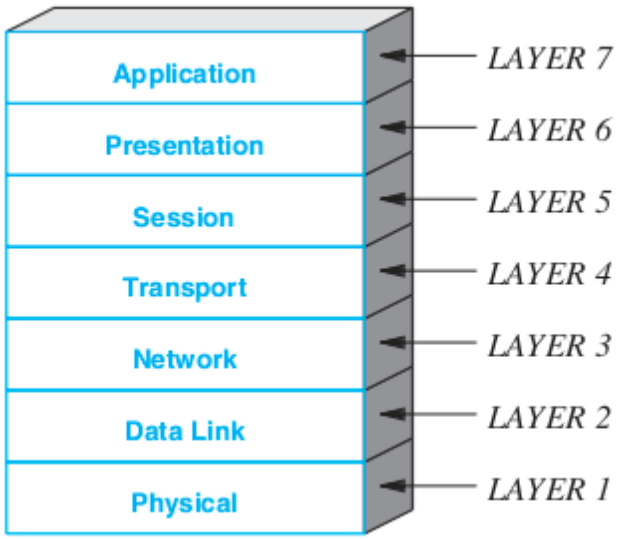
Commanders in the littorals must have the flexibility to face the challenges of the complex decision domain, while avoiding a decent into the inherently unpredictable domain of chaos or disorder. These decision makers can anticipate initial conditions, to some degree, based on a preconceived understanding of the mission, tacit knowledge gained from previous experiences, and initial or intended friendly force disposition. However, they cannot predict what impacts or influence the combination of environmental dynamics, enemy action and the movements of their own assets will have on their own C2 networks. Every mission or operation is different; therefore, decisions will require some novel combination of new or established techniques or tactics. The implementation of MANET in the littorals expands decision maker's ability to observe patterns of response through networked nodes. MANET also provide multiple courses of action for adjusting network performance through topology manipulation; the existence of multiple options, or "competing hypotheses," allows for "safe-to-fail" actions (Snowden, 2012). For example, a decision maker may have the ability to move several different nodes to bolster a mission-critical video feed and can observe the pattern of response to determine which action is successful. If observations indicate a different outcome than expected, he would have the flexibility to adjust and adapt to the situation.

3. Human-Network Interface Considerations

When considering the interface between a network operator and the network itself, it is important to understand how they interact. Modeling simplifies and decomposes complex systems through higher-level abstractions to allow a closer examination of the relationships, connections and influences that drive it. In many research fields, layered models are used to represent interrelationships between entities or theoretical strata within an entity. These are particularly useful when dealing with technology and the complexities of information flow at the human level. Military C2 is a fusion of both humans and information networks; understanding these models is the first step towards exploring the complex interface between the two.

The Open Systems Interconnection (OSI) 7-Layer model provides a reference framework for implementing communications protocols between nodes in a network. The International Standards Organization (ISO) provides a detailed description of this model in ISO/IEC 7498-1 (1996). This framework allows developers to have a common standard to guide the creation of more detailed interfaces. The layers in the OSI model represent seven related groups of functions, as depicted in Figure 7. While these functions are enabled by a multitude of applications, operating systems, technology and protocols; the 7-layer model allows the node interactions to be analyzed with a common frame of reference. Although this model illustrates the logical links between nodes at various levels, extant network connections only reside at the "physical" layer where bits are exchanged across transmission media.

Figure 7. OSI 7-Layer Communication Model



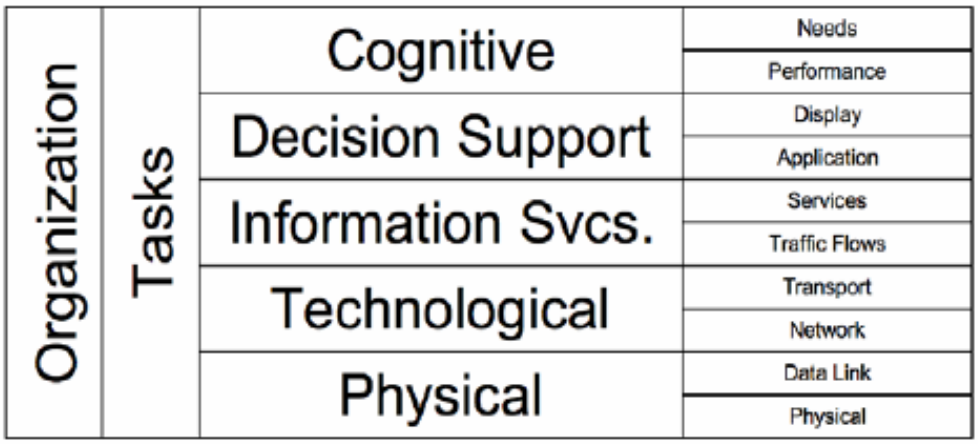
Source: Comer, D. (2014). *Computer networks and internets* (6th ed.). Upper Saddle River, N.J.: Pearson/Prentice Hall.

Bauer and Patrick (2004) assert that, despite the OSI model's success, it remains incomplete because it does not take human interaction into account. They propose an extension to the 7-layer stack to include "display" (how the user interacts via hardware, software and interfaces), "human performance" (perception, cognition, etc., that capture

user information processing capabilities and limitations), and "human needs" (needs being addressed via technology use). While the Human-Computer Interface (HCI) model refers to these as Layers 8, 9 and 10, it should not be confused with the Layer 8 adaptive network management C2 function discussed by Bordetsky and Hayes-Roth.

In order to understand how humans and information systems interact, it is necessary to explore how the models of these networked systems align to each other. Gateau (2007) accomplishes this by taking the combined HCI and OSI 10-layer stack (with minor modifications for clarity), and correlating each layer to the 3-layer Information Warfare model explicated by Alberts, Garstka, Hayes and Signori (2001). Alberts et al. (2001) categorize information effects on military operations into three domains—the physical, information, and cognitive domains. In this model, the physical domain represents the environments in which military forces operate and are connected by communications networks; data from the physical domain becomes contextualized, manipulated and shared in the Information domain. Human perception drives the creation of knowledge, understanding, and awareness, resulting in action through decision-making in the Cognitive domain. However, the granularity of this model does not adequately address the interfaces between each of these three domains (Gateau, 2007). The breadth of information domain remains relatively broad so it is appropriate to apportion it into addition layers by extracting technologies that are "rooted in the physical domain which process, store and manage data and information" (Gateau, 2007, p. 29) and decision support systems (DSS) and processes that shape information into something usable by humans and aid in its application. Shim et al. (2002) define DSS as "computer technology solutions that can be used to support complex decision making and problem solving" (p. 1). As a result, the Information Services Layer represents traffic flows and services as they pertain to data, information and explicit knowledge. It is also important to note the relationship between tasks and organizations in these models. Figure 8 illustrates that organizations are not just consumers of the information and decision support systems; they also interact with these systems through tasks and subtasks while concurrently controlling information flows and providing services within them (Gateau, 2007).

Figure 8. Organization-Information-Technology Model



Source: Gateau, J. (2007). *Extending Simple Network Management Protocol (SNMP) beyond network management: A MIB architecture for network-centric services*. Master's thesis, Naval Postgraduate School, Monterey, CA.

Gateau's work focuses on an SNMP-based approach to enhance network centric services at the Technological, Information Services and Decision Support layers of the Organization-Information-Technology model. This thesis is therefore a logical extension of his work with specific implications in the Decision Support and Cognitive domains as they influence maneuver in the Physical domain. The remainder of this section provides a cursory overview of theories used to support the analysis provided in Chapter IV.

a. Media Richness Theory

In their paper titled "Organizational Information Requirements, Media Richness and Structural Design," Daft and Lengel (1986) lay the foundation for what is now called Media Richness Theory (MRT). They propose of information processing at the organizational level is the reduction of equivocality and uncertainty. These terms are defined in Table 1. MRT is most commonly associated with human-to-human communications (e.g., email, text messaging, video-teleconferencing, face-to-face interaction) because humans have the "capacity to cope and respond to ambiguity" (Daft & Lengel, 1986, p. 26). From a military perspective, the operational environment drives information processing requirements as well as levels of uncertainty and equivocality (Bergin, Hudgens, & Nissen, 2011). Dynamic and hostile operational environments force

organizations to gather more information to adapt to the complexity of the environment that it faces (Daft & Lengel, 1986; Pfeffer & Salancik, 2003).

Table 1. Equivocality versus Uncertainty

Equivocality	Uncertainty
Ambiguity; the existence of multiple and conflicting interpretations of a situation	The difference between the amount of information required to perform a task and the amount of information already possessed by an organization

Adapted from Daft, R. L., & Lengel, R. H. (1986). Organizational information requirements, media richness and structural design. *Management Science, 32*(5), 554–571.

Daft and Lengel (1986), explain that media richness is the "ability of information to change understanding within a time interval. Communication transactions that can overcome different frames of reference or clarify ambiguous issues to change understanding in a timely manner are considered rich. Communications that require a long time to enable understanding or that cannot overcome different perspectives are lower in richness" (p. 560). We can consider this communication as exchange of information between a network management system and an operator or as information transactions in a higher-level social network; these are important considerations for decision makers processing and interpreting the tactical environment and analyzing information pertaining to the disposition and activities of their adversaries.

This is especially relevant for network operators in the littoral environment. Reducing uncertainty for dynamic littoral operations requires the collection and processing of information in a more time and space constrained operating area that would be experienced in blue water operations. In the littorals, sensors and nodes can provide adequate (sometimes overwhelming) amounts of information, but the effectiveness and utility of the increased information flows is limited by the decision maker's ability to cognitively process it in a timely manner. Additionally, elements of littoral complexity can amplify or obfuscate causes of network performance fluctuations that may be more readily discovered and addressed in other networks. DSS can reduce equivocality by

exposing causes of network instabilities or failure, node misconfigurations, faults and other issues to help network operators interpret and respond more quickly.

b. Cyber-Physical Systems

As sensors and systems continue to integrate into military C2 processes, as well as into civilian life through the "Internet of Things," cyber-physical systems will play an ever-increasing role in how information is interpreted and acted upon. Cyber-physical systems embody the integration of computational and physical capabilities that enable interaction with the physical world across cyber space (Baheti & Gill, 2011). The interactive contrivance between the cyber realm, including embedded systems and networks, and the physical world is a crucial area for innovation (Chun et al., 2010). Of particular importance is the extension of cyber-physical systems to include human interaction. The concept of cyber-physical-social systems (CPSS) is discussed by Liu, Yang, Wen and Zhang (2011) as a framework for self-synchronization in C2 systems that represents the convergence of cyberspace and organizational, cognitive and physical networks. This framework includes the human as a role player in CPSS, coupling humans and physical systems in the decision-making process rather than leaving the human "outside the system boundaries," as is the case with typical cyber-physical system implementation (Liu et al., 2011, p. 92). The integration and management of manned and unmanned platforms will require a paradigm shift in how a force's actions affect, and are impacted by, the dynamic nature of physical and cyber clutter within the battlespace.

c. Human-Systems Integration

Human-Systems Integration (HSI) represents a system-level approach to enabling synergistic interaction between the human and the system to improve task effectiveness as a function of system and human performance. The central notion of HSI is that the human element is a key consideration in all phases of a system's life cycle. Dolgov and Hottman (2012) characterize the human element as the "perceptual abilities, cognitive capacity, situational awareness, and the ability to perform under stress or in high cognitive-demand situations contribute to the effectiveness of the human–machine system" (p. 173). The HSI approach is a topic of much discussion in the realm of

unmanned systems development. The application of HSI is this area primarily focuses on analyzing how humans interact with unmanned systems to increase the operational effectiveness of the system and operator acting as a team. Dolgov and Hottman (2012) add that "displays, controls and the overall human-machine interface design are the component of HSI that compliments the user" (p. 174). Developers can gain insights on how to design systems that will better serve the end user and increase the efficiency of their interactions by focusing on satisfying user's ergonomic needs, information flows and processing capabilities in situations of high stress or other cognition-affecting scenarios.

4. Unmanned Platform Integration

The ongoing development of new, highly capable unmanned platforms for air, surface, subsurface and land operations is dramatically changing how military operations are conducted. Advances in processing capabilities and computing power are bringing increased autonomy to the rapidly growing unmanned systems arena. However, the integration of these platforms in maritime operations still faces unresolved questions. Unmanned systems can fill lingering operational capability gaps; reducing threat exposure faced by manned platforms in hostile environments. In many cases, they are "the preferred alternatives especially for missions that are characterized as dull, dirty, or dangerous" (U.S. Department of Defense, 2013, p. 20). The Unmanned Systems Integrated Roadmap (U.S. Department of Defense, 2013) outlines the DOD's 25-year vision for the technical development and integration of unmanned aerial, land and maritime systems. While this document does take a network-centric approach, it primarily discusses the future roles of unmanned vehicles as satellite communications gateways/relays but essentially ignores their integration into a network as MANET nodes.

The potential benefits of unmanned aerial vehicles functioning as communications relays are relatively well researched. Rothal, Davis and Marlatt (2015) provide a sampling of NPS unmanned systems-related theses, reports and papers, 35 of which discuss their use as relays in different environments. Everly and Limmer (2014) provide a multi-objective cost-effectiveness analysis of 15 aerial platforms and nine

communications payloads. Quincy et al. (2010) discuss a novel command and control architecture for UAV relays in an high-value unit (HVU) defense role.

There is, however, significantly less research regarding the implications of their participation as active nodes in a dynamic MANET architecture from a network operations perspective. Richard (2009) applies self-tuning adaptive control algorithms to optimize UAV position to support communications links between multiple ground antennae. Richard's approach uses physical layer network performance as guidance input for UAVs and provides a basic example of how cyber-physical maneuver can realize enhancements in a tactical MANET with UAVs. The current deployment construct for unmanned assets like the MQ-4C Triton and MQ-9 Reaper limit their usefulness in dynamic littoral tactical environments. These larger UAVs are typically high demand/low density assets, retained as theater-/national-level services and requested to support specific missions as available. Smaller UAVs launched from maritime platforms, like MQ-8B Fire Scout and RQ-21A Blackjack, can provide on-demand flexibility for tactical commanders. For example, the smaller size of the RQ-21A allows it to maintain a minimal launch and recovery footprint on the deck of a ship, but its payload capacity is adequate enough to carry electro-optical/infrared sensors and small synthetic-aperture radars (Butler, 2012). This payload capacity also provides an opportunity to integrate more advanced communications payloads, like MANET systems. The question is: Who contributes this information into the planning and execution of operations in the littorals, and what tools enable the same?

The Joint Concept for Command and Control of the Joint Aerial Layer Network (Joint Chiefs of Staff, 2015c, p. 1) provides a vision for the future of UAV relays as an "augmentation and extension of tactical networks using a variety of communications capabilities that will support operations in challenging or degraded communications environments within a Joint Operations Area (JOA)." This goal of JALN is to provide a high capacity backbone for information transfer across a JOA, functioning as a router and gateway to allow disparate C2 systems to access the Department of Defense Information Network (DODIN). The DODIN is the DOD's global network infrastructure that provides warfighter access to information capabilities and support by "collecting,

processing, storing, disseminating and managing information" (Joint Chiefs of Staff, 2015a, p. 65). As a future concept, this document makes significant assumptions regarding the C2 of JALN. One example of this is the assertion that "network planning and control processes and systems will accomplish network management" (Joint Chiefs of Staff, 2015c, p. 3). This, in effect, minimizes the significance of network planning and management in the employment of dynamic networks topologies. Overall, the focus of this concept is the support of the Joint Force Commander (JFC) at the operational level and assumes the need for mission prioritization to address high-demand/low-density issues.

Unmanned systems in other domains can also increase the flexibility and effectiveness of network-enabled operations in the littoral environment. Advances in unmanned underwater vehicle (UUV) technologies can bring new underwater sensing network capabilities to the littorals. Ongoing development of Large Displacement UUVs (LDUUV) at Naval Undersea Warfare Center (NUWC) Keyport will bring persistent littoral undersea surveillance into A2/AD environments. Additionally, unmanned surface vehicles (USV), like SeaFox, have long endurance and high payload capacity that enable them to serve as cross-domain network nodes and are highly suitable for a multitude of missions (National Defense Research Institute, 2013). The Unmanned Systems Integrated Roadmap does not discuss the use of UGVs as a potential network augmenter; however, experimentation conducted by CENETIX indicates potential usefulness in that role.

B. NETWORK MANAGEMENT

> When deciding to throw a party, no one thinks at first of the effort that goes into planning the party, the logistics, the cleanup—you think of the party itself and how much everyone will enjoy it. And certainly no one throws a party just for the sake of the work that it involves, but for the fun they expect out of it. This is not unlike the situation with networking and network management. (Clemm, 2006)

Clemm's amusing analogy provides some insight into the challenge of network management as an afterthought in many organizations. The importance of network management is receiving increasing attention due to the growing emphasis on networked systems within organizations. Network management becomes more relevant as the

complexity of the network increases (Clemm, 2006). Additionally, network and network management task complexity can increase as a result of the types or numbers of nodes involved (Frye & Cheng, 2010). The DOD's NCW transformation highlights the importance of networks as an integral part of modern military operations, but the technical challenges of integrating new technologies in dynamic operating environments demand active and effective network management.

Ren and Li (n.d.) define network management as "a service that employs a variety of protocols, tools, applications, and devices to assist human network managers in monitoring and controlling of the proper network resources, both hardware and software, to address service needs and the network objectives." Network management can be viewed in three functional groups: network provisioning, network maintenance, and network/service operations (Shenoy, n.d.). Network provisioning pertains to network planning and design, typically concerning fixed network infrastructure. Network maintenance includes network installation, repairs and trouble ticket administration. However, the majority of day-to-day network management effort supports network operations. Network management systems (NMS) provide the tools used to monitor, configure and provision network resources, as well as a host of other functions and are integral to the operations of any IT enabled organization. Subramanian (2010) discusses network operations as it relates to a Network Operations Center (NOC) using the OSI FCAPS model as a foundation.

1. FCAPS

As part of the OSI network management model, ISO delineated five network management application categories for user-oriented applications that are necessary for NOC operations—fault, configuration, accounting, performance, and security management (FCAPS) (Subramanian, 2010). These categories provide a framework for network management applications that enable network operators to monitor and maintain network functionality. The FCAPS functional model provides a useful model for discussing network management at higher levels of abstraction. Table 2 provides an overview of the five functional areas of the OSI FCAPS model.

Table 2. FCAPS Overview

Fault Management	Detecting, isolating, fixing and recording errors that occur inside the network.
Configuration Management	Maintaining accurate information on the configuration of the network (hardware and software) and controlling parameters that relate to its normal operation.
Accounting Management	User management and administration, as well as accounting and billing for the use of the resources and services.
Performance Management	Maximizing network performance relative to Quality of Service (QoS) provisioning and to parameters such as resource utilization, delay, jitter and packet loss.
Security Management	Ensuring security and safety in the network.

Adapted from: Boutaba, R., & Polyrakis, A. (2001). Projecting FCAPS to active networks. In Proceedings of Enterprise Networking, Applications and Services Conference. doi: 10.1109/ENTNET.2001.981995

While all of these areas are pertinent to network management, approaches to fault and configuration management must evolve to enable effective management of tactical networks.[2] Fault management functions rely on network monitoring tools in order to manage and react to alarms indicated abnormal behavior in the network (Clemm, 2006). This process relies on a centralized management system to detect faults and locate their root causes so problems can be resolved quickly. Configuration management commonly entails middle- to long-range activities pertaining to planning and managing changes in software, hardware, and network provisioning. Configuration management also includes network topology discovery and mapping, as well as the setup of configuration parameters in management agents and systems (Subramanian, 2010). This is particularly relevant to tactical networks with constantly changing and intermittent participants.

[2] Security management is of utmost importance to the network management of any DoD network but is outside the scope of this thesis. Accounting management is not directly applicable to tactical network operations.

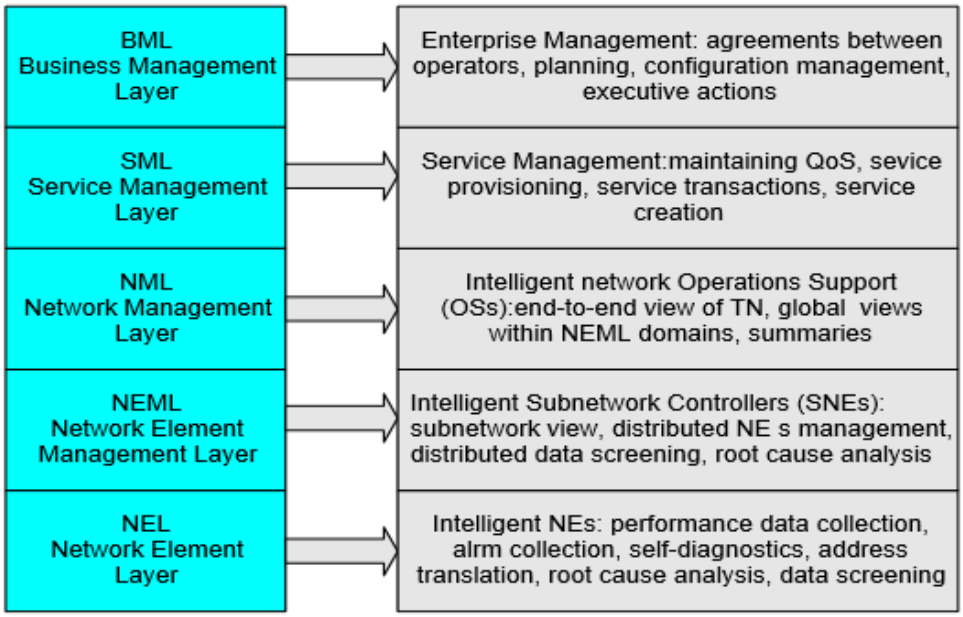
2. Telecommunications Management Network (TMN) Service Architecture

The TMN architecture was originally developed in 1986 as a means of addressing the interoperability of proprietary telecommunications management systems from a network and network element level, as well as the higher level service functions of an organization (Subramanian, 2010).

The TMN model is represented in five layers. At the lowest layer, *network elements* refer to any piece of hardware on the network that can be monitored and managed (Gateau, 2007). The *Network element management* layer contains applications that manage network elements and may be vendor specific or proprietarily designed for a specific device. The *network management layer* provides the end-to-end view of the network in terms of performance, bandwidth, flow control, etc., and is vendor agnostic (Subramanian, 2010). The *service management layer* focuses on the ability of the network to provide services residing on that network. Finally, the *business management layer* is concerned with overarching operational requirements of the organization (e.g., planning, personnel, customer satisfaction, etc.)

Gateau (2007) offers that, despite TMN's "dizzyingly complex" (p. 34) governance mechanisms and documentation, the TMN service architecture provides an appropriate level of abstraction for broader application. This thesis leverages the TMN service model in this manner. Bordetsky and Hayes-Roth (2006) provide some clarity to the TMN service model (depicted in Figure 9) by explicating on functions of network operations at different layers.

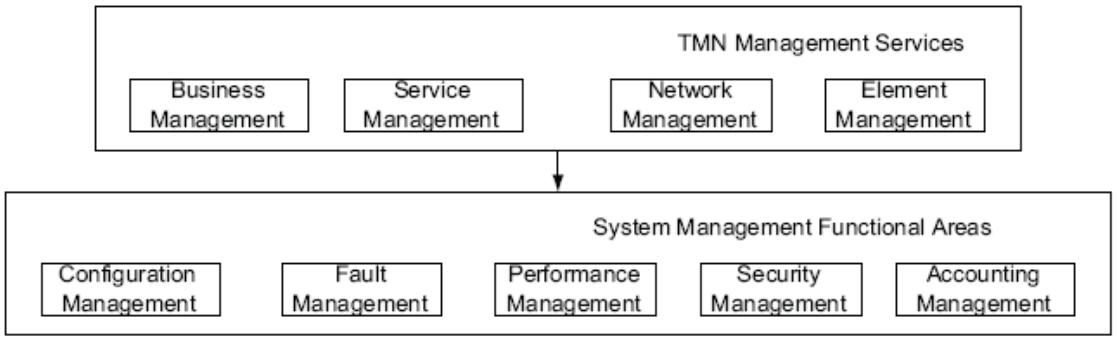
Figure 9. TMN Architecture of Network Operations Layers



Source: Bordetsky, A., & Hayes-Roth, R. (2006). Hyper-nodes for emerging command and control networks: The 8th layer. In Proceedings of 11th International Command and Control Research and Technology Symposium. Retrieved from http://www.dodccrp.org/events/11th_ICCRTS/html/papers/127.pdf

The TMN service model builds on OSI management principles and the five management functional areas of FCAPS. Hierarchically, the TMN management services "invoke" the system management functions (FCAPS) in order to manage the network according to operational objectives and service requirements. Figure 10 depicts this relationship.

Figure 10. TMN Management Services and Management Functional Areas



Source: Subramanian, M. (2010). Network management: principles and practice. Safaribooksonline.com. Pearson Education India. Retrieved from http://techbus.safaribooksonline.com/book/networking/network-management/9788131727591

It is important to note that the FCAPS management functions typically consist of siloed groups of applications that provide decision support to dedicated network operators within a NOC. Bordetsky and Hayes-Roth (2006) describe the role of the "Network Facilitator" who collects and interprets information from disparate DSS sources to determine overall network effectiveness. In other words, an array of network management information must be ingested and interpreted by human operators and becomes a pool of tacit knowledge that is refined through the acquisition of additional knowledge and feedback.

3. Adaptive Network Management

Mobile ad-hoc networking provides the foundation connecting nodes at the tactical edge to achieve NCW-compliant integration (Peacock, 2007); however, achieving robust adaptability in the face of environmental and enemy interference is critical to the successful implementation of the MANET. Koch and Golling (2015) assert that the A2/AD threat challenges NCW doctrine and that disruptions to heavily relied-upon communications links, (e.g. satellite communications), can degrade a force's decision-making capabilities. Their response, dubbed "Robust Network Centric Warfare," recommends increasing adaptability from the physical layer (OSI layer 1) through the application layer (layer 7), via adaptable communications networks, protocols, and information exchange requirements.

However, focusing on adaptability improvements for network communications is not adequate. The management of these networks must also be considered. Characteristics of mobile ad hoc networks require constant reconfiguration based on network performance feedback. Bordetsky and Hayes-Roth (2006), introduce the concept of 8th-layer adaptive network management as an extension of the 7-layer OSI model that uses *hypernode* elements capable of adapting network behavior and performance based on dynamic conditions and mission requirements. Gateau (2007) explores the hypernode concept and provides an SNMP-based Management Information Base (MIB) architecture for network-centric services. Increases in computing power and performance enable the use of proactive management algorithms. Current NMS capabilities provide for autonomously testing network performance and detecting QoS deterioration and abnormalities prior to network failure, as well as correlating and recognizing alarm patterns (Clemm, 2006). However, the implementation of intelligent, adaptive self-control within networks requires further work in the realm of Case-Based Reasoning and other memory mechanisms to enable 8th-layer NOC functionality at the node level.

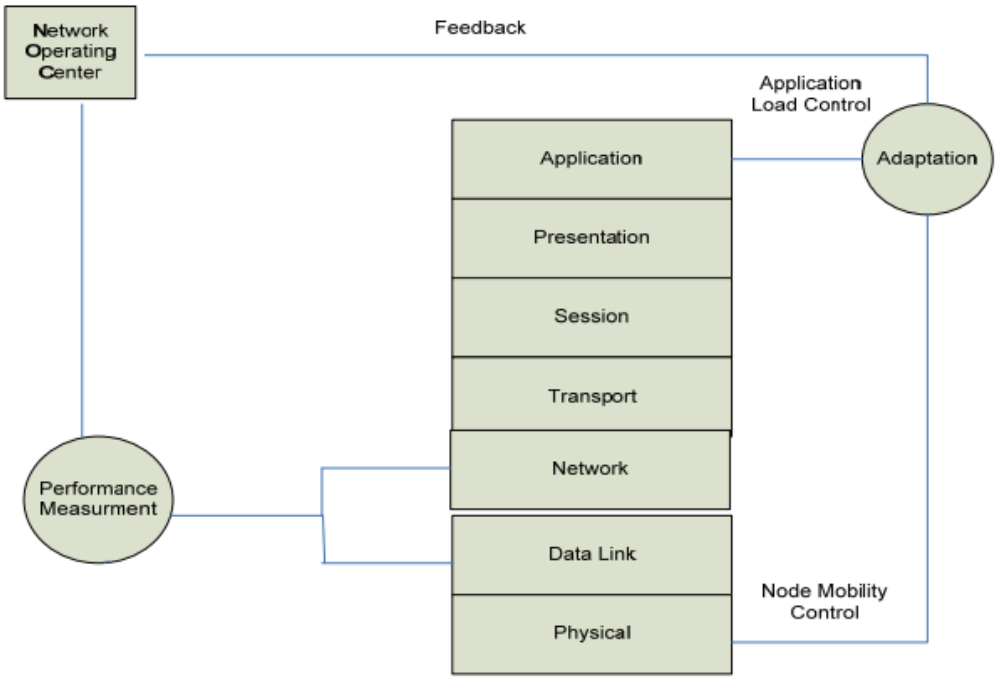
A complementary approach to adaptive network management is provided by Bordetsky and Netzer (2010). In their discussion of the CENETIX Tactical Network Testbed, they highlight the fundamental challenge of adaptive management in tactical networks:

> We typically measure the performance of self-forming tactical networks by capturing network (IP) or data link (wireless) layer packet flows. However, in most practical cases we can't bring our feedback controls directly to the same layer. The most feasible options available to the tactical NOC crew or local commanders would be limited application load controls (less video, still images only, voice only, etc.) at the top most applications layer, or node physical location (mobility) control at the lowest physical layer. (Bordetsky & Netzer, 2010, p. 20)

To their point, the movement of nodes to maintain LOS or improve signal strength and the manipulation of application load within the network indicate the increased significance of configuration management in MANET, addressed in a later section. Therefore, the combination of application load management and node mobility form the

nexus of active MANET configuration management. Figure 11 illustrates how a NOC using this adaptive management approach would interact with the network.

Figure 11. Layers of Adaptation for Maritime MANET

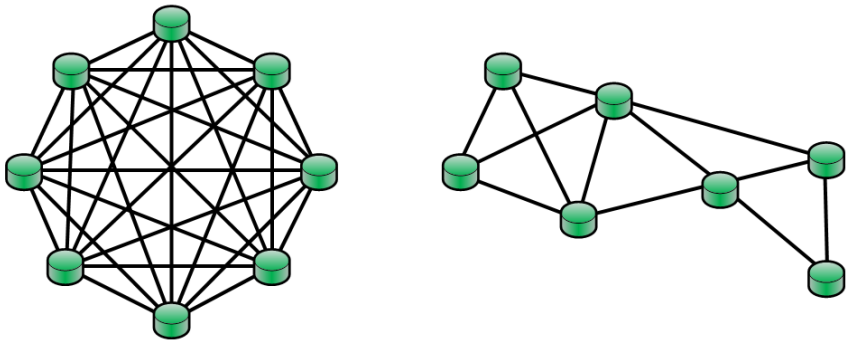


Source: Bordetsky, A., & Netzer, D. (2010). Testbed for tactical networking and collaboration. *The International C2 Journal*, *4*(3). Retrieved from http://www.dodccrp.org/files/IC2J_v4n3_B_Bordetsky.pdf

4. Mesh Networks

The description of a mesh network as flexible, self-forming, self-healing, and eventually self-organizing originates from graph theory: a pure mesh network topology is described as a complete or fully interconnected graph (Bordetsky et al., n.d.). Fully connected mesh topologies provide redundant interconnections and fault tolerance within a network but are expensive and difficult to accomplish. Partial-mesh topologies provide a realistic approach to redundancy and interconnectivity for dynamic nodes by providing multiple alternative routes without the cost of a full mesh topology, as shown in Figure 12.

Figure 12. Full Mesh versus Partial Mesh Topology



From the computer and information networking perspective, mesh networking could take place at any layer of network functionality and can be understood in terms of the OSI 7-layer hierarchy. Bordetsky et al. (2015) explain:

> At the lowest physical layer populated by moving assets such as ships, vehicles, and their antennas, it could be viewed as a directional or physical network of highly dynamic components. At layer 3, the Internet layer, it is a typical IP space mesh of logical paths, which are alternated and recalculated by routers, subject to changing conditions in node mobility as well as application performance. At layer 7, a similar mesh behavior could be viewed as a complete graph of application flows, in which the flows are swiftly adjusted in response to a changing situational awareness/decision support process in a shared C2 cycle. (p. 3)

While mesh networking can manifest at various layers, approaches can be categorized into physical layer implementation (e.g., radios), the network itself, and the social networks of users interacting with them.

a. MANET

The characteristics of MANET make them highly suitable for networks at the tactical edge. MANET technologies allow users to collaborate more easily and attain better situational awareness than ever before—"this increased situational awareness is the cornerstone enabling capability for the NCW tenets of cooperative engagement and self-synchronization" (Peacock, 2007, p. 13). The multi-hop nature of MANET allows the extension of networks beyond line-of-sight and in areas where fixed infrastructure is not

in place. Initial overhead and resource requirements are reduced due to the decentralization and dynamic routing capabilities of MANET systems. Ongoing development of Delay Tolerant Networking (DTN) seeks to overcome issues associated with disconnected or intermittent connectivity, allowing nodes to store and forward packets of information opportunistically between disconnected nodes (Team CASA, 2014).

MANETs are different from Wireless Mesh Networks (WMN) in a number of ways. Although they are both multi-hop approaches to networking, key differences include reliance on infrastructure, destination of traffic flows, and mobility (Sichitiu, 2006). WMN require a multi-tiered infrastructure consisting of users, mesh routers, and gateways with most traffic across exchanged across the network via user-to-gateway interface. Connectivity across WMN usually occurs at layer 3 as a result. Network traffic on MANETs can include gateways for access outside of the network but the majority of network traffic is peer-to-peer (layer 2). The ad-hoc nature and dynamic node mobility of MANET mean that most instances are effectively partial mesh topologies.

b. Technologies

Research on near-shore mesh networks has great potential to increase tactical advantage of naval forces operating in the littorals. Pathmasuntharam et al. (2008) analyze low-cost, high-bandwidth solutions for ship-to-ship/shore mesh networking as a communication path to replace or complement satellite communications in near-shore commercial maritime applications. Their research focuses primarily on safety-of-navigation, providing two-way voice/data communications and Internet access to ships transiting narrow channels and close to shorelines (Pathmasuntharam et al., 2008). The International Telecommunications Union–Radiocommunication Sector (ITU-R) report M.2202 (2011) discusses additional research regarding commercial maritime broadband wireless mesh networks. In this report, ITU-R outlines various hardware and protocol challenges faced by maritime mesh networks but maintains that the approach is feasible given further efforts to standardize mesh protocols for maritime usage (Radiocommunication Sector of International Telecommunication Union, 2011). While

these papers primarily focus on WMN, the key issues they address and the challenges they identify are also relevant to MANET implementation for maritime networks.

As these standards continue to be developed, several communication technology companies have attempted to bridge the gap between the commercial and tactical realms. Companies such as Trellisware, Harris, and Persistent Systems have developed proprietary MANET technologies directly intended for military operations in tactical environments ashore and afloat.

A prime example of modern MANET technology is the Wave Relay system produced by Persistent Systems. Wave Relay is a suite of intelligent MANET radios that includes compact handhelds and larger units for vehicles or fixed sites. The experimentation outlined in Chapter III leveraged this technology as a surrogate representing more powerful MANET systems that could be implemented in littoral tactical networks.

CENETIX research utilizes three Wave Relay radio models for experimentation: the Man-Portable Unit (MPU) 3; the MPU4; and, the Quad Radio router. Table 3 provides a comparison of these systems.

Table 3. Quad Radio, MPU3, and MPU4 Specification Comparison

	FIPS 140-2 Level 2	IP67?	Suite B	No of Radios	No of Ethernets	Mpbs UDP Throughput (20 Mhz Channel)	Mpbs TCP Throughput (20 Mhz Channel)	Input Voltage (VDC)	Power (Avg/Max) 2 W Radio	Dimensions (L x W x H inches)
Quad	✓	✓	✓	4	5	37	27	8-48	8 / 55	8.5 x 6 x 2
MPU3	✓	✓	✓	2	2	37	27	10-48	5.7 / 25.2	5.0 x 4.7 x 1.8
MPU4	✓	✓	✓	1	2	37	27	8-48	4.2 / 16.5	7.8 x 3.0 x 1.5 with battery

Adapted from: Persistent Systems. (2014). Wave relay capability specifications sheet. Retrieved February 7, 2016, from http://www.persistentsystems.com/pdf/WaveRelay_ Capability_SpecSheet.pdf

CENETIX researchers found the greater power and functionality of the Quad Radios and MPU3s apposite for fixed mounting on larger vessels and structures ashore. The compact size of the MPU4 allowed mobile operators aboard smaller vessels to access SA tools and reach-back elements through the MANET.

5. MANET Management

The management of tactical networks presents a much different problem set than that faced by managers of contemporary fixed networks. Tactical networks typically require information exchanges for short durations, whereas administrative networks require continuous operation for indefinite periods (Joint Chiefs of Staff, 2015b). Kidston and Kunz (2008) assert that, as compared to contemporary networks with high data rates and fixed topologies, maritime MANETs "engender a novel combination of management challenges" (p. 164). These challenges include:

- Commercial NMS are not directly compatible with MANET systems;
- The heterogeneity of tactical communications systems affects interoperability;
- Rapid reconfiguration is a persistent requirement during MANET operation due to changes in mission requirements and operational needs;
- Disconnected, intermittent and limited communications environments results in high error rates and variable bandwidth;
- Limited access to skilled network operators;
- Dynamic network topologies and related difficulties due to MANET mobility;
- Security concerns due to the nature of RF communications.[3]

SNMP is the primary means of network performance monitoring used by commercial NMS (Subramanian, 2010). Many MANET systems lack SNMP functionality; instead, these systems utilize Application Program Interfaces (API) for access to system performance information. However, the diverse ecosystem of

[3] Addressing network security and system vulnerabilities is beyond the scope of this thesis. However, they are of the utmost importance, especially when considering a tactical environment with sophisticated adversaries who can inject, manipulate or otherwise interfere with communications in the RF spectrum.

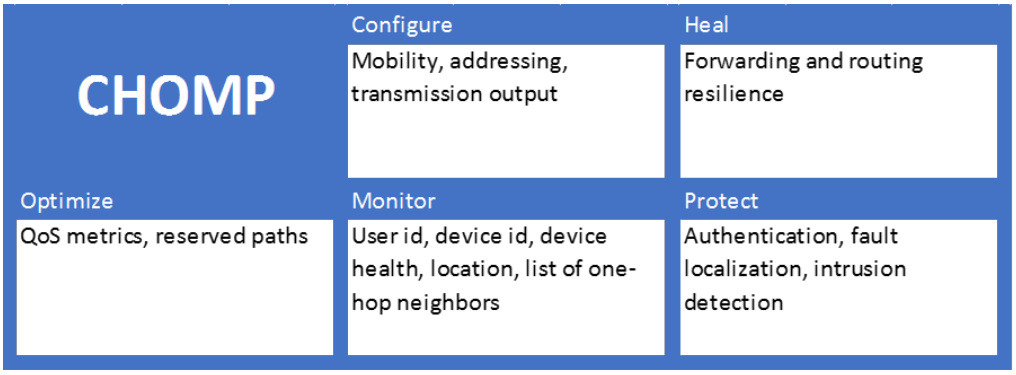
communications systems that will be operating in the tactical environment requires an NMS that can consolidate, normalize and process information from multiple source types that can include API, SNMP and other network management communications schemas.

The dynamism and fluidity of tactical networks challenge traditional network management paradigms; however, the fundamental underpinnings of network management models are useful for tailoring network management systems and approaches to meet operational needs. The FCAPS model used for network management for traditional wired networks is relevant; however, management services must adapt to compensate for the challenges of the maritime environment.

Network life cycle phases of wired networks are linear with each phase separated in time. Using CISCO's Network Management Reference Architecture (2008) as an example; the phases of the Prepare, Plan, Design, Implement, Operate, and Optimize (PPDIO) life cycle can be reduced to two—Design and Operational. Accounting and security aside, configuration activities typically occur during the design phase. Whereas, the principle line of effort in the operational phase of wired networks goes toward fault management and performance optimization. The constantly changing and adaptive nature of MANET forces these functions to occur contemporaneously. Management functions now become intertwined and interconnected; changes in configuration immediately manifest in changes in performance and variations in performance drive network re-configuration.

The domains of MANET management must reflect the shift in emphasis from a disjointed, primarily linear approach to a more integrated model. Based on the FCAPS framework, Kidston and Kunz (2008) offer the following critical management areas: configure, heal, optimize, monitor, and protect—subsequently referred to as the CHOMP model, illustrated in Figure 13.

Figure 13. CHOMP Model



Adapted from: Kidston, D., & Kunz, T. (2008). Challenges and opportunities in managing maritime networks. *Communications Magazine*, *46*(10), 162–168. doi: 10.1109/MCOM.2008.4644135

The functions of configuration and monitoring are both well engrained in traditional wired-network management approaches (Kidston & Kunz, 2008). However, the effects of mobility, resource scarcity/constraints, and both physical and cyber clutter are unique to the realm of tactical networks. Kidston and Kunz (2008) go on to explain with regards to healing and optimization that:

> network and application self-(re)configuration…involves managing the entire life cycle of the network from initial configuration (initialization) to the application of new operational rules (evolution), to reconfiguration of devices upon failures (robustness),[4] and finally, discovery and configuration of new (and related) devices as they become available (adaptation). (p. 165)

It might be inferred that healing and optimization therefore belong to an overarching category of "re-configuration" which supports the evolution, robustness and adaptation of the tactical network after initial configuration, although they are described by Kidston and Kunz as discrete, complementary activities.

The discovery and configuration of new nodes as they join the network poses potential technological challenges (e.g., out-of-band configuration) but also provides opportunities for network scalability. It may be possible to enhance network coverage by

[4] The reconfiguration of failed devices referred to by Kidston and Kunz can also refer to interfaces, application services, or other similar elements.

taking advantage of friendly, MANET-equipped vessels transiting the operating area even if they are not organic to the AFP or group of assets under the Commander's purview.

This approach provides a unique, relevant and useful model when considering the management of maritime MANET. These critical management areas provide the foundational elements for the development of a robust and holistic NMS solution for the tactical maritime MANET. This thesis uses these management areas as a framework and for further analysis in Chapter IV.

6. Network Operations Tools Used For CENETIX Experimentation

CENETIX offers a unique venue for the exploration of littoral-centric C2 and mesh networking concepts. The ability of the CENETIX testbed to extend its cyber-physical environment through a global collaborative network offers a plethora of tools, including network management, plug-and-play man-machine interfaces, and data collection capabilities to experiment sites around the world. Another benefit of using an extension of the testbed environment is the ability to capture and replay experiment scenarios to enable seamless continuity in the transfer of research knowledge to subsequent testing and CONOPS development.

CENETIX field experimentation exploring littoral network management in 2015 leveraged three systems for the deployment and management of tactical networks: CENETIX SA Server, Wave Relay Management Interface, and the CodeMettle Network Service Orchestrator.

a. CENETIX SA Server

CENETIX experimentation relies on organically developed web services accessible via the CENETIX web portal. The CENETIX SA Server is an organically developed situational awareness sharing system, purpose-built to provide the CENETIX NOC with a common operating picture during field experiments. Using Google Earth as a platform, the CENETIX SA Server stores mobile device locational information accessible from the CENETIX portal in Keyhole Markup Language (KML) format. This

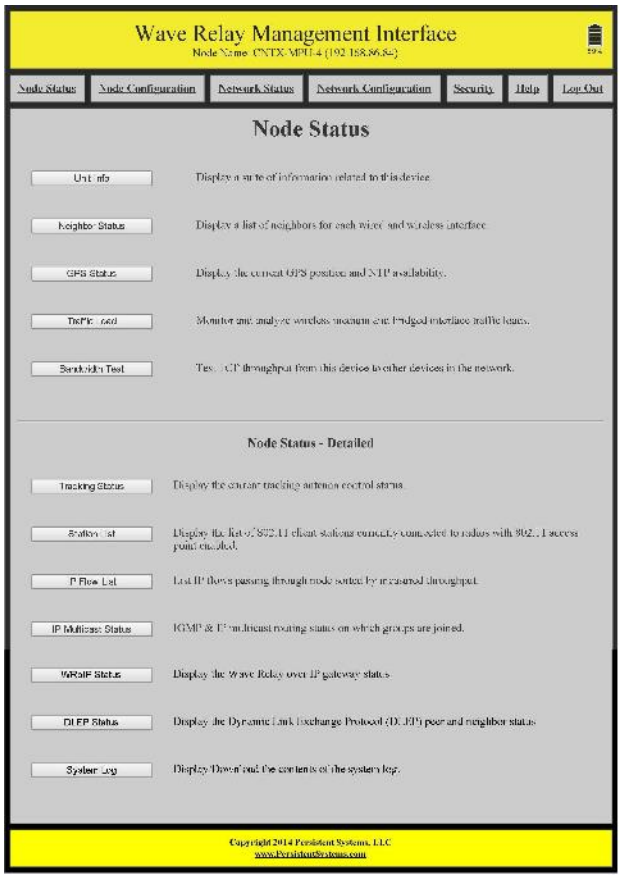
allows KML subscribers to view the locations of these devices in Google Earth and supports the use of track history and scenario replay available in the program. Radios within the network are configured to transmit Cursor-on-Target (CoT) messages to the CENETIX SA Server. The GPS locational data contained in the CoT messages is stored and processed at the CENETIX SA server. This location data is subsequently used to plot 3-D location information for each node. The locational data stored on this server integrates GPS data transmitted directly to the server from other mobile devices on the testbed. PLI stored by the SA Server is visible to subscribers as track history and can be replayed from the CENETIX Web Portal. In addition to the SA Server, the CENETIX web portal also hosts Observer Notepad for text notation, chat, and file sharing, as well as the VC1 Video Conferencing tool for streaming video, used during all experiment phases. Data generated locally flows through the CENETIX Resource Portal to remote CENETIX servers located on the NPS campus for display/dissemination. Figure 14 shows the CENETIX Resource Portal tools in use.

Figure 14. CENETIX Resource Portal Tools

b. Wave Relay Management Interface

The Wave Relay Web Management Interface enables users to configure and monitor radio units via a web browser. All radio functionality is only accessible through the web interface due to the lack of external Wave Relay radio controls. The Web Management Interface sorts configuration and monitoring functions into five tabs: node status, node configuration, network status, network configuration, and security. The Wave Relay Management Interface is shown in Figure 15.

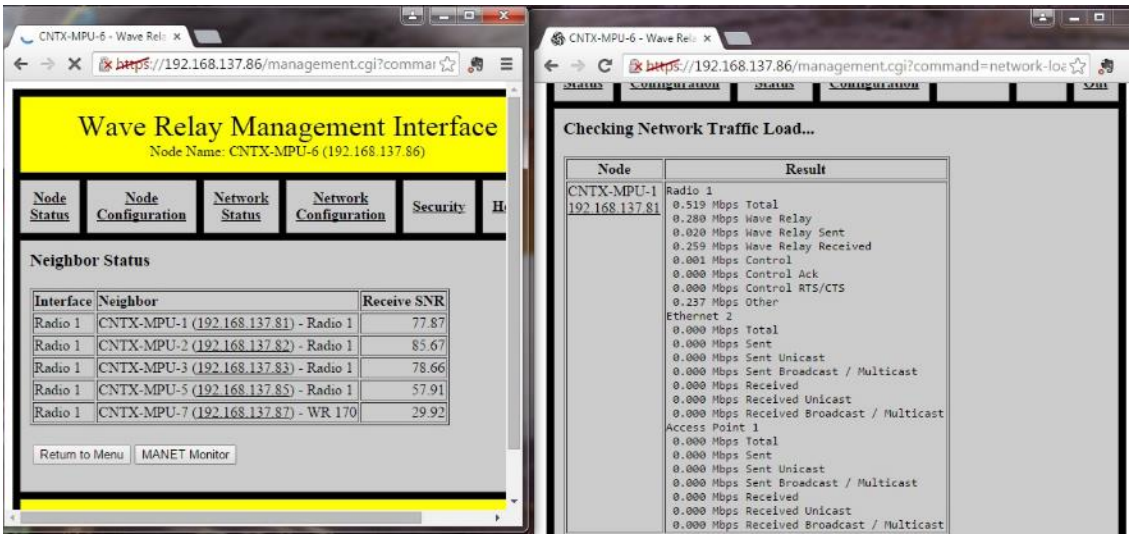
Figure 15. Wave Relay Management Interface



The "node status" tab provides node-specific information for the specific radio that the user is accessing based on the IP address used. This includes hardware and software information, the status of connected neighbor nodes, GPS status, traffic load, and other node monitoring information. This information is consolidated under the

"network status" tab for all radios—information from each radio is collected, combined and displayed textually on one page. Figure 16 gives an example of the network performance information visible on the Wave Relay Management Interface.

Figure 16. Examples of Network Performance Information Available on Wave Relay Management Interface



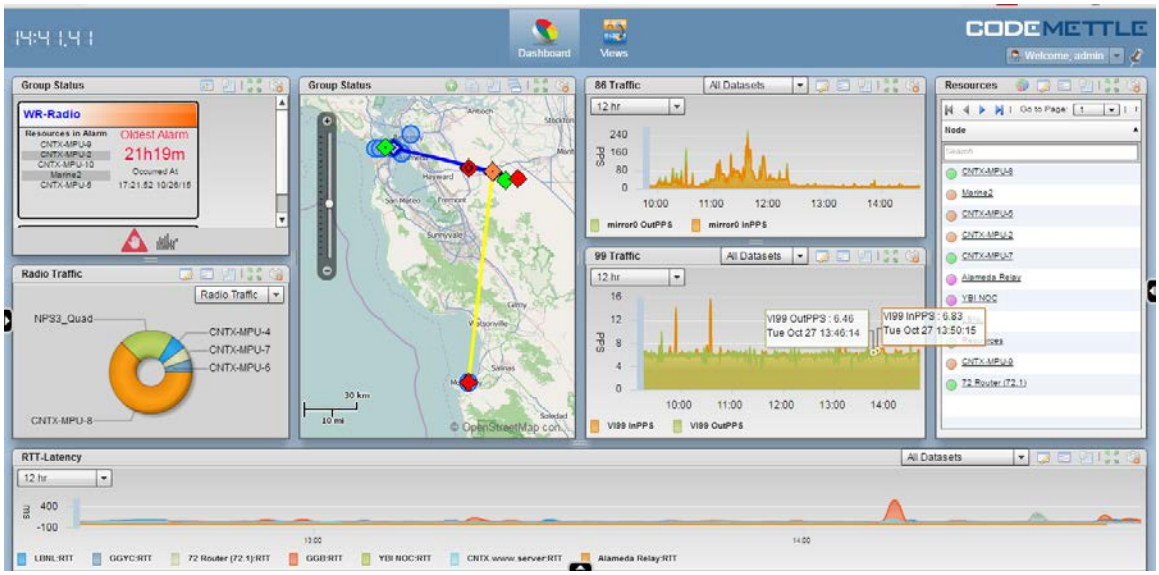
"Node configuration" provides options for managing the accessed node and includes settings for MANET routing, radio, access point, GPS, Ethernet, and a host of other configuration functionalities. The "network configuration" tab allows users to change the nodes included in network-wide configuration changes; changes to default settings for all radios in the network can also be adjusted on this tab.

Security functionality is also accessible through the web interface. The "Security" tab provides the ability to set a key, configure encryption settings, zeroize the key on the radio, and enable tamper detection (this zeroizes the radio if its enclosure is compromised).

c. CodeMettle Network Service Orchestrator (NSO)

The CodeMettle system provides a network agnostic approach to the management of heterogeneous networked assets, including the standards and protocols used by those assets. The NSO is an open-source, open-architecture system that is rapidly deployable across any hybrid network and offers a browser and mobile-based user interface that is fully configurable. Network performance information is collected, normalized, and stored in an SQL database. The unified dashboard allows for network data from any management functional area to be displayed, textually or graphically, on a single interface. The CodeMettle dashboard tailored for use during CENETIX experimentation is shown in Figure 17.

Figure 17. CodeMettle Unified Network Management Dashboard



THIS PAGE INTENTIONALLY LEFT BLANK

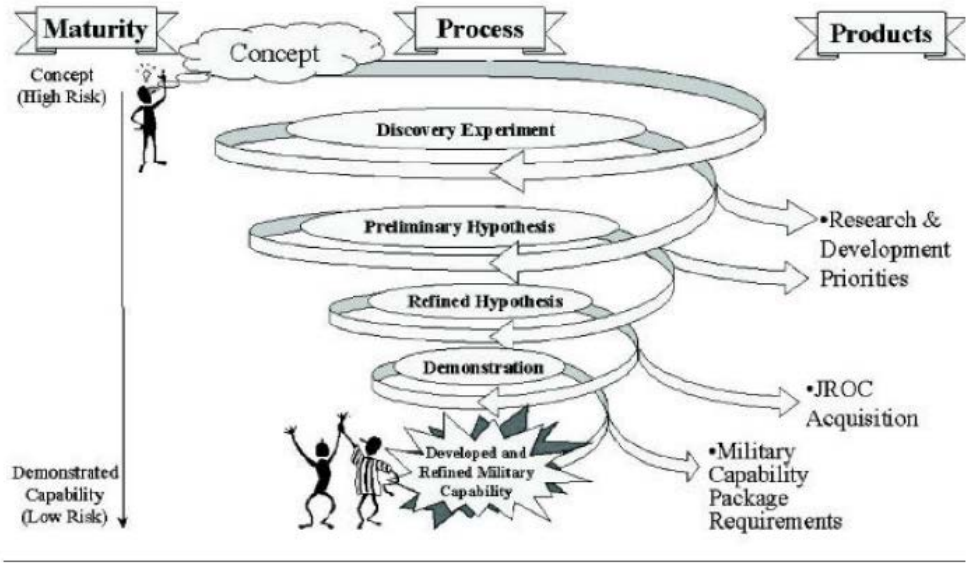
III. RESEARCH DESIGN

Two CENETIX field experiments were conducted in 2015. The NATO Maritime Interdiction Operations Training Center in Souda Bay, Crete hosted a June 2015 research event. A second experiment in October 2015 took place in San Francisco Bay, California. The experiments leveraged mesh-networking technologies to enable the sharing of situational awareness in combined and interagency operations. Although these experiments focused on MIO and CWMD operations, lessons learned from these events are broadly applicable to operations throughout the littoral domain.

While the overall research design took place across the execution of two disparate experiment events, each experiment featured key elements that contributed to subsequent testing. The CENETIX MIO experiment in June 2015 focused on locational data sharing across a local mesh network architecture connected to the CENETIX testbed through a local gateway and included unmanned systems functioning as network relay nodes. The October 2015 CENETIX CWMD experimentation expanded the local mesh network architecture in a littoral environment. A key objective for this experiment was the management and monitoring of the hybrid mesh network. This hybrid architecture leveraged a combination of mesh networks and satellite communications systems to integrate unmanned ground and undersea vehicles as data producers within the CENETIX testbed ecosystem.

The planning and execution of these field experiments provided the critical underpinnings for the incremental development of littoral mesh network management operations. In line with the experiment campaign process explained in the *Code of Best Practice for Experimentation* by Alberts (2002), the goal of this research is to frame an initial concept for littoral mesh network management operations and to provide an overview of the CENETIX discovery experimentation. Figure 18 illustrates the logical steps of an experiment campaign as a concept matures into a demonstrated military capability.

Figure 18. Experiment Campaigns



Adapted from Alberts, D. S. (2002). *Code of best practice: experimentation*. Washington, DC: CCRP.

Several research phases executed over the course of these two events analyzed the potential of mesh network management operations in the littoral domain. They were broken up into the following phases:

Phase 1—Souda Bay, June 2015

1. Configure, bench test, and deploy mobile ad hoc networking technologies in an experimentation testbed environment;
2. Implement and test situational awareness / data-sharing software using 3D visualization (e.g. CENETIX SA Server, Wave Relay KML);
3. Integrate unmanned systems as relay nodes in the network;
4. Implement and test Wave Relay Management Interface capabilities for MANET management in a littoral environment.

Phase 2—San Francisco Bay, October 2015

5. Integration of unmanned systems as data producers in the network;
6. Tailor network management software to provide a decision-support component for controlling physical layer topology and performance (CodeMettle);

7. Test network management software within the hybrid mesh testbed architecture.

These steps provide the basic outline for the methodology and results presented in this thesis. Exploration of unmanned system applications and mesh network orchestration/management systems in this research are predicated on the implementation of a littoral mesh network architecture. Additionally, experimentation with systems intended to improve situational awareness contributed to the development of the mesh network orchestration concept.

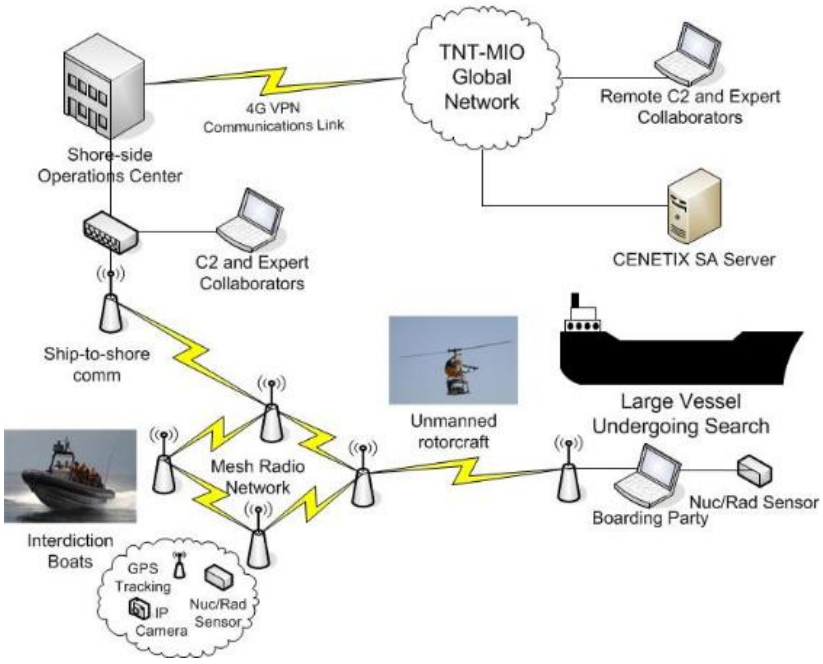
A. CENETIX-NATO MARITIME INTERDICTION OPERATIONS TRAINING CENTER (NMIOTC) EXPERIMENTATION (JUNE 2015)

The June 2015 experiment focused on shared situational awareness among partner nations as part of a coalition force conducting maritime interception operations in Souda Bay, Crete. In this case, situational awareness information was comprised of Position Location Information (PLI), voice, chat, and video feeds generated by each patrolling vessel. Figure 1 illustrates the overall scheme of maneuver for the experiment. Vessels from countries "A" and "B" were equipped with mesh radios attached to Panasonic CF-52 laptops or handheld mobile devices. Using these devices, users were able to access real-time track information, chat and video streams that provided them the ability to quickly identify and intercept a target vessel crossing a notional jurisdictional boundary.

1. Mesh Network Deployment

For the purposes of CENETIX testing and experimentation, Persistent System's Wave Relay MPU-3 and MPU-4 Radio units provided the basic mesh architecture. The high throughput, reliability, and compatibility with other CENETIX testbed elements prompted the selection of these systems. The CENETIX research team developed a general CONOPS and scheme of maneuver for each of the experiments. These plans guided the generation of network diagrams. Network topologies supported several disparate test sets to provide the required flexibility to support needs of each system. Figures 19 depicts the basic network topology for the June 2015 experiment.

Figure 19. MIO Experiment Basic Network Topology



Configuration and network monitoring for each node was available through the web browser-based Wave Relay Management Interface. Initial Wave Relay radio implementation required manual configuration of individual radios. For example, radios had to have matching security keys in order to join the mesh network. Additionally, several radios were set up to serve as wireless access points allowing mobile devices to share data and access the CENETIX-designed Observer's Notepad collaboration tool. Once radio configuration was complete, a full connection test was conducted between each radio to ensure proper setup. Channel selection for radio frequencies was limited to the 2312–2507 MHz range due to equipment constraints. However, the specifications for this Persistent Systems WR-RAD-12 radio model allowed the use of 2 watt transmit output power, which improved radio performance during experimentation. All other radio configurations were set to default.

2. Situational Awareness and Data Sharing

In order to leverage the CENETIX web portal tools, each radio was configured to transmit Cursor-on-Target (CoT) messages to the CENETIX SA Server. The GPS locational data contained in the CoT messages was stored and processed at the CENETIX SA server. This location data was used to plot 3-D location information for each node.

As stated in Chapter II, the locational data stored on this server integrates GPS data transmitted directly to the server from other mobile devices on the testbed. PLI stored by the SA Server is visible to subscribers as track history and can be replayed from the CENETIX Web Portal. Users were able to access SA Server tools, and utilize other CENETIX web portal functionality; these included Observer Notepad for text notation, chat, and file sharing, as well as the VC1 Video Conferencing tool for streaming video. These tools were used during all experiment phases. Data generated locally flowed through the CENETIX Resource Portal to remote CENETIX servers located on the NPS campus for display/dissemination. Laptop nodes used Virtual Private Network (VPN) connections to access this information from the Portal through the Internet Connection Sharing (ICS) gateway. VPN tunneling enabled direct access to streaming video feeds and CoT data visualizations from the CENETIX servers. Figure 20 shows the CENETIX Resource Portal tools in use.

Figure 20. CENETIX Resource Portal Tools

The Wave Relay Management Interface provides a similar situational awareness tool to the one hosted by the CENETIX SA Server. User nodes connected directly to the Wave Relay mesh network can subscribe to a KML feed via the Management Interface. When viewed using Google Earth, node PLI is visible as well as the mesh data links connecting each node (depicted in Figure 21). The Wave Relay Management Interface does not store PLI so track history is not available to the user. The colors of the visible data links indicate performance based on SNR, however there is no legend correlating SNR level to the respective color indicator:

1. Red = poor
2. Yellow = acceptable
3. Green = good
4. Blue = excellent

Figure 21. Wave Relay Management Interface KML Viewed in Google Earth

3. Unmanned System Integration (Relay Node)

The CENETIX testbed environment is well suited for testing the integration of unmanned systems in littoral operations. CENETIX experimentation in June 2015 explored several use-cases for unmanned vehicles within a littoral operating environment, focusing on their use as relay nodes. Coordination of these experiments came from the CENETIX Network Operations Center located at NMIOTC Headquarters in Souda Bay, Crete, approximately 2 miles northwest of Nisida Souda Island. This allowed investigators the ability to monitor network operations and information flows through different phases of each experiment. Additionally, the testbed provided a centralized C2 location for unmanned system testing.

Unmanned aerial vehicles in the June 2015 experiment demonstrated the use of aerial assets to bolster mesh network coverage over geographic obstacles in the littoral environment. This network relay link allowed boarding teams on the Hellenic Navy's training vessel (ex-Aris) to have reachback connectivity for the nuclear detection sensors being used to search the target ship. Figure 22 depicts the relative location of the UAV.

Figure 22. Relative Location of Hellenic Navy UAV Flight Path

System design for the Hellenic Navy UAV required direct control of the aircraft from a ground station through a point-to-point RF link. However, the aircraft was outfitted with an MPU-4 radio that served as a connecting node between radios located on the southern portion of Nisida Souda Island and on the ex-Aris training vessel. Users on onboard ex-Aris were not in LOS of the NOC, so the island and UAV relays provided connectivity for testing in that location. The small size of the UAV (illustrated in Figure 23) allowed its launch from the pier adjacent to ex-Aris.

Figure 23. Hellenic Navy UAV Fitted with MPU-4 Radio

Once airborne, the UAV executed a circular holding pattern directly over the northern end of Nisida Souda Island. This holding pattern allowed the radio to relay network traffic between nodes on ex-Aris and simulated Unmanned Ground Vehicle (UGV) nodes on Nisida Souda Island. UAV testing was limited due to mechanical failures onboard the aircraft.

Simulation of UGV relay nodes also facilitated the exploration of unmanned systems operating in tandem to improve mesh network performance. Two stationary nodes were placed on accessible structures located at high points along the southern edge of the island. The placement of these nodes was conceptually based on areas accessible to UGVs deployed to provide semi-fixed relay coverage. Physical location of East and West Relays are visible in Figure 24.

Figure 24. Relative Locations of East and West Relays

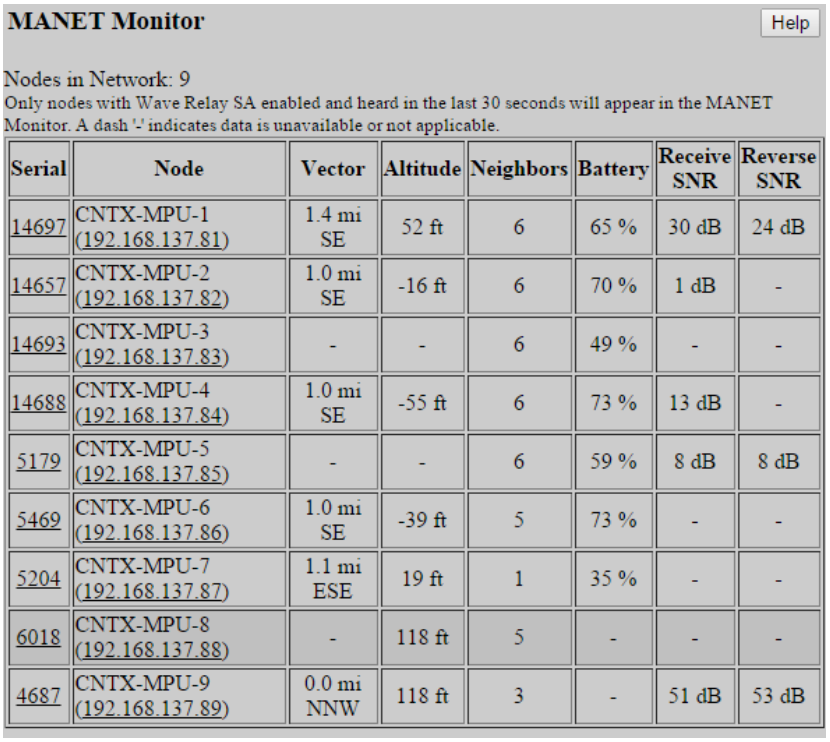
Due to the mechanical failure of the UAV, boarding teams in ex-Aris were not able to directly connect into the mesh network relays on Nisida Souda Island or at NMIOTC. To compensate for this, two ship nodes were directed by the NOC to maneuver into position to act as relay nodes. These nodes are labeled as “CountryA” and “CountryB” in Figure 25. Identifying an adequate location for the repositioned nodes was accomplished using the Wave Relay Management Interface and the Google Earth KML to view and verify connectivity was reestablished. Once the nodes were in place, links to ex-Aris were restored; however, link quality remained relatively degraded.

Figure 25. Maneuvering of Relay Nodes to Reestablish Connectivity to ex-Aris

4. MANET Management with Wave Relay Management Interface

The Wave Relay Management Interface provides access to a variety of network performance data, including network traffic load at each node, signal-to-noise ratio (SNR) between nodes, and other information. Researchers in the NOC utilized a combination of the tools available on the Management Interface in conjunction with the 3-D visualization and VC1 video conferencing tool. This was due to the inability of the Wave Relay Management Interface to monitor application performance or notify NOC personnel if network performance was degraded or contact with network nodes was lost. As a result, the NOC relied primarily on the "MANET Monitor" function (shown in Figure 26), as well as visual cues from the Google Earth WR KML and VC1 video feeds that indicated network performance issues.

Figure 26. Wave Relay Management Interface MANET Monitor



MANET Monitor Help

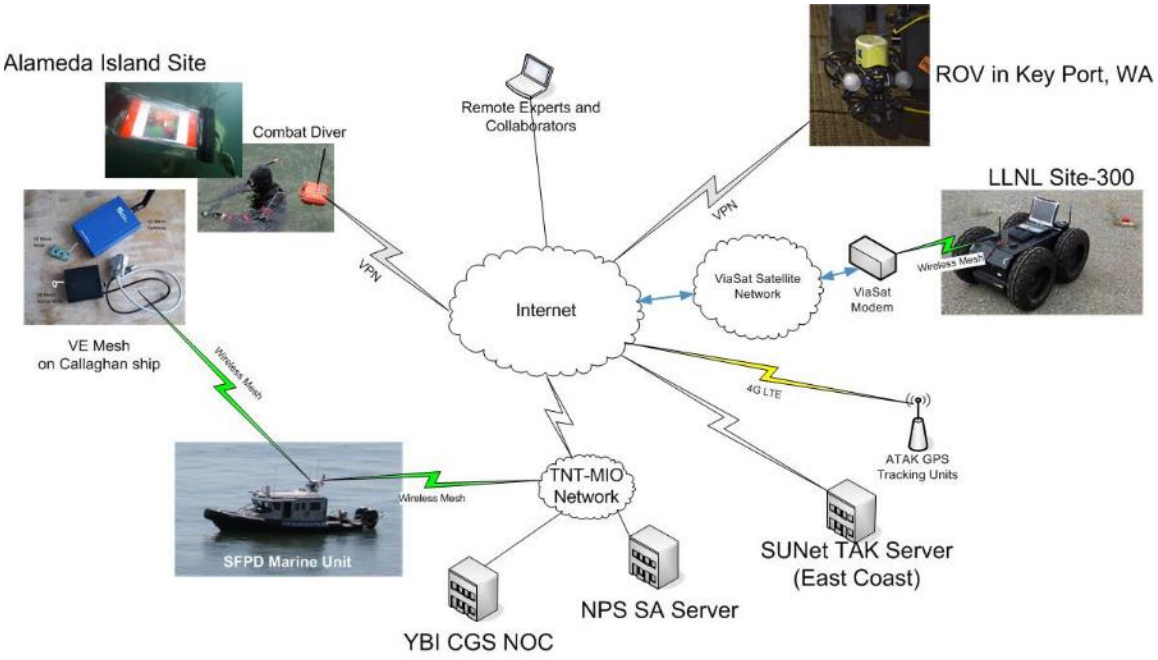
Nodes in Network: 9
Only nodes with Wave Relay SA enabled and heard in the last 30 seconds will appear in the MANET Monitor. A dash '-' indicates data is unavailable or not applicable.

Serial	Node	Vector	Altitude	Neighbors	Battery	Receive SNR	Reverse SNR
14697	CNTX-MPU-1 (192.168.137.81)	1.4 mi SE	52 ft	6	65 %	30 dB	24 dB
14657	CNTX-MPU-2 (192.168.137.82)	1.0 mi SE	-16 ft	6	70 %	1 dB	-
14693	CNTX-MPU-3 (192.168.137.83)	-	-	6	49 %	-	-
14688	CNTX-MPU-4 (192.168.137.84)	1.0 mi SE	-55 ft	6	73 %	13 dB	-
5179	CNTX-MPU-5 (192.168.137.85)	-	-	6	59 %	8 dB	8 dB
5469	CNTX-MPU-6 (192.168.137.86)	1.0 mi SE	-39 ft	5	73 %	-	-
5204	CNTX-MPU-7 (192.168.137.87)	1.1 mi ESE	19 ft	1	35 %	-	-
6018	CNTX-MPU-8 (192.168.137.88)	-	118 ft	5	-	-	-
4687	CNTX-MPU-9 (192.168.137.89)	0.0 mi NNW	118 ft	3	-	51 dB	53 dB

B. CENETIX COUNTER-WMD EXPERIMENT (OCTOBER 2015)

October 2015 experimentation integrated knowledge collected from the June 2015 experiment and explored distributed knowledge sharing in a Counter-WMD scenario. A primary focus of this experiment was the use of distributed assets across the CENETIX backbone network, including unmanned ground and underwater vehicles. The Operations Center located at the USCG Station Yerba Buena in San Francisco Bay provided a centralized location for operational C2 and network management. This location made it a suitable surrogate for a shipboard Littoral Operations Center. Internet connectivity through the USCG network provided access to the CENETIX network. Additionally, a Wave Relay Quad Radio router with a sector antenna was installed on the communications tower adjacent to the building. This mesh radio connected maritime assets in San Francisco Bay to the Operations Center and acted as a gateway to enable their access to the CENETIX Network. The basic network topology for the San Francisco Bay experiment is shown in Figure 27.

Figure 27. SF Bay CWMD Experiment Basic Network Topology



1. Unmanned Systems Integration (Data Producer)

The use of unmanned systems in the October 2015 experiment shifted from network relays to data producers within the littoral testbed network. This experiment focused on the use of ground vehicles for site exploitation and radiological/nuclear material detection, as well as the use of underwater vehicles for search and diver cueing.

The CENETIX RMP-400 Unmanned Ground Vehicle (UGV) was equipped with an Adaptable Radiation Area Monitor (ARAM) radiological/nuclear detection device provided by Lawrence Livermore National Laboratory (LLNL). UGV control relied on waypoint entry using a remote interface operated from the Yerba Buena Island NOC. Once the waypoints were selected and the "mission execute" command sent, the UGV navigated to each of the defined waypoints. Video streaming provided the operator with near real-time progress updates. Figure 28 shows the portal-based control interface for the RMP-400.

Figure 28. RMP-400 Mission Control Interface

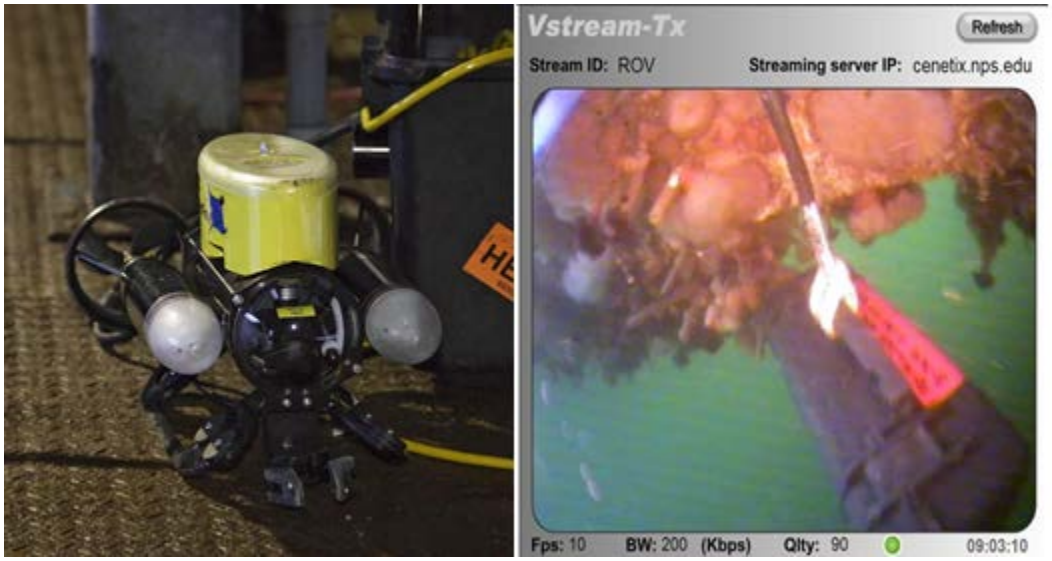
Using a live radiological source from Lawrence Livermore National Laboratories (LLNL), detection data collected by the ARAM system were processed by the RMP-400's onboard computer. These data were automatically posted to the CENETIX server for reachback analysis. Server connectivity was established through a local Wave Relay network connected to a ViaSat terminal gateway. Figure 29 shows the RMP-400 in action at LLNL Site 300.

Figure 29. RMP-400 Equipped with ARAM Sensor

CENETIX partnered with Naval Undersea Warfare Center (NUWC) Keyport, Washington to test the underwater diver communication system designed by NPS. This is the first CENETIX experiment exploring the concept on an unmanned underwater vehicle providing data directly to divers operating underwater, without the need to return to the surface for data connectivity. At the time of the October 2015 experiment, systems allowing 360-degree underwater video collection with onboard UUV systems were still under development. NUWC Keyport's VideoRay remotely operated vehicle (ROV) provided a surrogate platform.

A pelican case, representing a parasite box containing illicit materials, was submerged adjacent to the NUWC Keyport pier. ROV operators were directed by the NOC to search for the parasite box. Once found, imagery of the parasite box was transmitted directly to divers in San Francisco Bay. Video taken by the ROV was piped through the CENETIX Resource Portal video streaming tool. Divers viewed screenshots of the video feed, received text commands, and were able to upload pictures to the NOC through the CENETIX-developed Networking-by-Touch (NbT) system. This allowed the NOC to direct divers to confirm the presence of the parasite box and provide instructions for subsequent actions from reachback experts. Figure 30 shows the video stream from the NUWC Keyport ROV.

Figure 30. NUWC Keyport ROV and Video Stream through CENETIX Portal



2. CodeMettle Network Service Orchestrator Deployment

Littoral operations are supported by an integrated network of manned and unmanned platforms and systems. These nodes are connected via a hybrid network including satellite, radio, and Ethernet. However, while the network nodes are well integrated, often the management of these nodes is disparate based on technology, function, or vendor. That is, network operators currently must use multiple management tools to address different aspects of the network and must manually aggregate the data to create a single picture of the network, or non-real-time situational awareness.

In collaboration with CodeMettle LLC, network services and elements resident in the CENETIX testbed environment enabled the development of a tailored, unified network management dashboard. The CodeMettle Network Service Orchestrator (NSO) dashboard provides centralized awareness and management of network assets, combining geo-location information, IP traffic performance, and the ability to better visualize dynamic mesh topologies.

Situational awareness information was required by the NOC not only for the tactical MANET, but also the CENETIX backbone that supported the experiment. As CodeMettle was informed of the exercise 5 calendar days before the experiment, the

agility of the tool's deployment was an added factor influencing the experiment's results. The following sections will describe how CodeMettle NSO was integrated into the experiment and obtained, processed, and presented real-time network situational awareness.

a. Data Acquisition

The first step in designing the unified dashboard interface was to determine what information is relevant at the tactical level from a cyber-physical maneuver perspective and how to present it to the user. The open-architecture design of the CodeMettle NSO allows the integration of disparate network management protocols into a single interface.

The foundation of network management and common situational awareness is data acquisition from the network and the equipment. CodeMettle created simple data "translator" scripts to access data from the hybrid network and normalize the disparate data from different technologies and vendors into a common data model. Prior to the experiment, NPS and CodeMettle investigators outlined various requirements for the NSO dashboard that included:

- Node Details
- Geographical display of node PLI
- Graphical representation of data links between nodes
- Radio performance information (e.g. SNR)
- IP traffic load and network quality
- Node faults
- Track history and dashboard replay

While the CodeMettle NSO can access data using any API, for this experiment the following interfaces were used to collect data supporting these requirements:

- SNMP: IP infrastructure including routers, switches, servers
- Web-queries: MANET radios
- Network probes: link latency and quality

An umbrella management tool must be flexible and should handle network data in the most efficient way. For example, while Wave Relay MPU-4 radios have an onboard management API that allows routers to be configured and monitored using an HTTPS interface, CodeMettle obtained data from the Wave Relay Management Interface web page served by the radios. With limited time and operators' experience interpreting the web pages, probing the same pages eliminated the step of processing an unfamiliar data format. Only when this data was normalized in a common model was intelligence able to be gained via data correlation and visualization.

Development of the CodeMettle NSO dashboard did not include integration of radio configuration, over-the-air-rekey (OTAR), or over-the-air–zeroize (OTAZ) capabilities. However, these functions are available through the Wave Relay API and could be integrated into the CodeMettle NSO. As the first implementation of this system in the CENETIX testbed, the CodeMettle NSO map display was limited to 2-D graphics, however, 3-D map visualization could be incorporated in future testing.

b. Data Processing

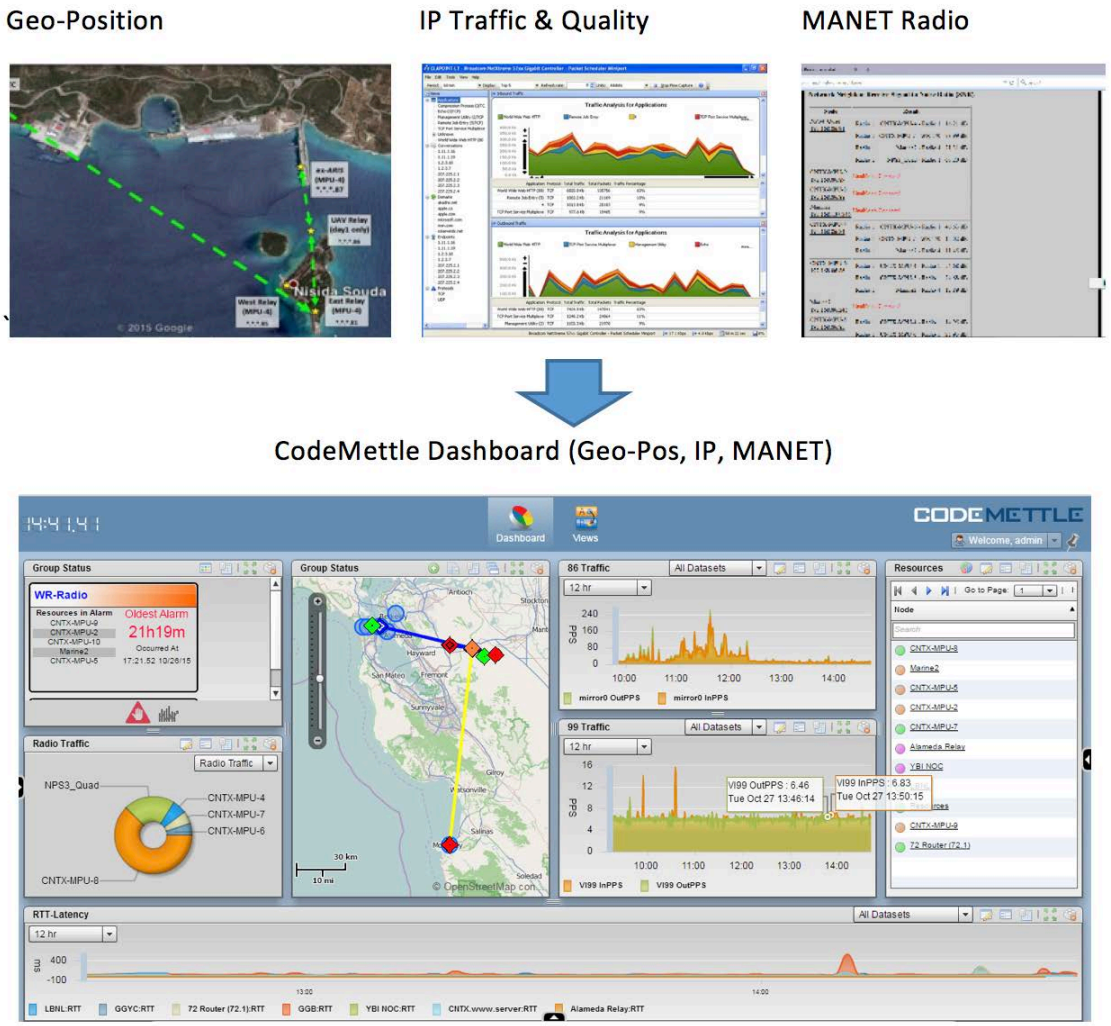
The raw data must be processed and correlated based on the network and mission's situational awareness requirements. For the October 2015 experiment, the primary objective was to correlate geographic position of assets to network quality during the tactical maneuvers, and secondarily to monitor the health and quality of the supporting backbone network. To accomplish this, CodeMettle correlated geo-positioning data from the MANET radios with network quality and traffic through the IP infrastructure and radio network.

Using the CodeMettle NSO, researchers conducted network discovery to identify active nodes and interfaces. The testbed contained both Wave Relay and standard network equipment such as laptops, computers, and routers. The CodeMettle system consolidated network performance, configuration and fault information into a single, unified and intuitive dashboard. Users were able to reconfigure the dashboard to display information pertinent to operations and mission requirements.

c. Data Visualization

Using configurable dashboards and input from the researchers, CodeMettle NSO presented real-time situational awareness of the tactical and backbone network. In past experiments, correlating geo-position with network performance required three separate tools that were consolidated into the CodeMettle platform for the October 2015 CWMD experiment. The dashboard depicted in Figure 31 was created for the CENETIX backbone network that supported the experiment.

Figure 31. CodeMettle Unified Network Management Dashboard



A tactical dashboard was also created to provide situational awareness during the exercise (shown in Figure 32). This dashboard correlated geo-position to network performance in the dynamic MANET network as the manned and unmanned systems manuvered for the exercise. The bottom left and bottom center dashboard components are an excellent example of transform complex network data into intelligence with intuitive visualization. With a glance, the network operator can visualize the geo-position of network nodes in the bottom-left map and easily determine quality of connectivity to neighbors nodes in a radar chart; the network operator can easily tell which nodes have degraded connectivity and inform them to move closer to a network node to increase quality. Access to this visualization enabled the proactive use of node placement and resource allocation to support network requirements.

Figure 32. CodeMettle MANET Tactical Management Dashboard

For this experiment, the focus was on MANET operations between six U.S. Coast Guard Auxiliary boats and a San Francisco Police maritime patrol. The MANET enabled users' access to CENETIX testbed tools, streaming video, and collaboration across the network. Changes in network performance were immediately visible on the dashboard as the topology changed due to node mobility. This information was visible on the map display that also provided a visual representation of network topology. In addition, radio and interface traffic indicated which nodes were generating the most flow across the network. Ultimately, the NSO interface provided this information in a much more robust and richer fashion than extant tools and bridged the gap between MANET and traditional network management functions. Despite a determined effort by the CodeMettle team, data collection and dashboard replay functionality for post-mission or post-failure analysis were not available for testing.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. EXPERIMENT OBSERVATIONS AND ANALYSIS

The contributions of this chapter are twofold. First, this chapter provides significant observations and key takeaways from the June and October 2015 experimentations. Additionally, this chapter touches on the littoral scenario introduced in Chapter I and analyzes the implications of CENETIX field experimentation results on this vignette through the lens of the concepts and theories outlined in Chapter II.

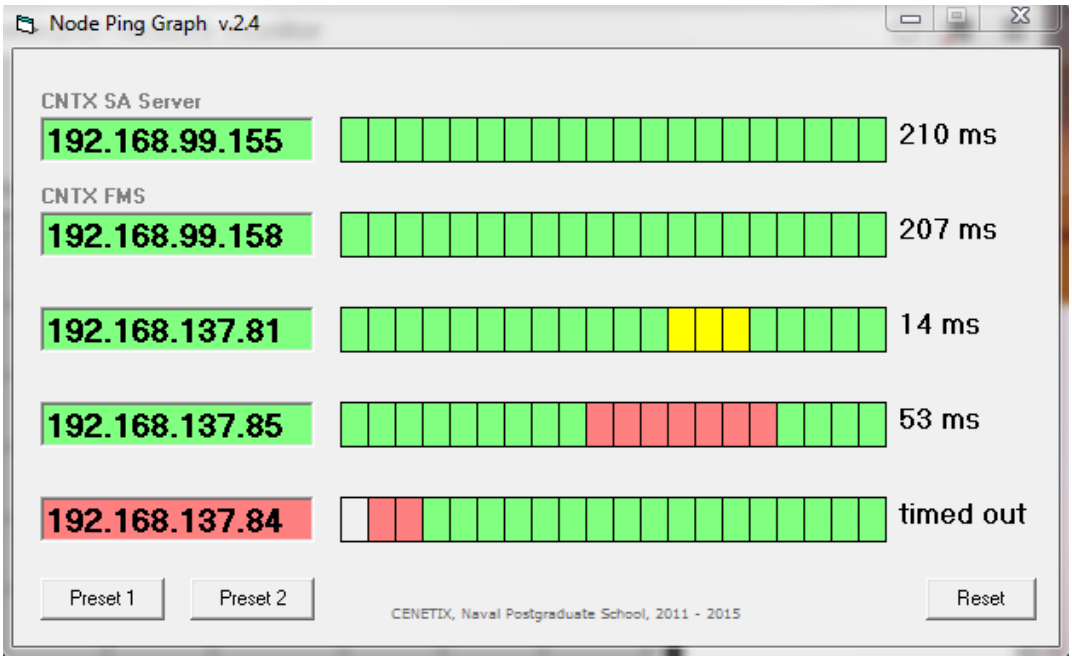
A. CENETIX NMIOTC EXPERIMENTATION (JUNE 2015) OBSERVATIONS

As discussed in Chapter III, the June 2015 experiment focused on shared situational awareness among partner nations as part of a coalition force conducting maritime interception operations in Souda Bay, Crete. This involved the deployment and management of a Wave Relay MANET that included the use of unmanned vehicles as network relays. Network operators were able to monitor network performance via the Wave Relay Management Interface. The Wave Relay and CENETIX SA Server were used to provide network operators with situational awareness information relevant for network management. This section outlines the observations and conclusions based on the June 2015 NMIOTC experiment.

It was observed during this experiment that Wave Relay's onboard management interface provided relevant MPU node configuration and node/network performance information. However, this information was located on several different tabs of the interface and only available in text format. The lack of a unified interface with illustrative graphics hampered the network operator's ability to quickly identify, correlate and assess changes in network performance. Additionally, the Wave Relay Management Interface lacks fault detection functionality: issues within the network were not explicitly visible to the network manager. Mesh radio performance during the experiment was limited due to a radio-antenna mismatch—two radios were identified to have incompatible antennas following the experiment. This impacted radio performance, however, these issues were not apparent to the NOC during the event.

The Wave Relay Management System is limited solely to Wave Relay radio nodes. Additional tools were necessary to monitor the performance of attached devices and other elements of the network. Conventional network management systems are not compatible with MANET technologies, so network managers were limited to basic ICMP functions (e.g., pinging) to verify connectivity with these devices (Figure 33).

Figure 33. Node Ping Graph Monitoring Network Connectivity for both MANET and Non-MANET devices



In addition to monitoring ICMP functions, network operators visually gauged the status the network connection by watching the quality of video being transferred through the CENETIX Portal via the VC1 video conference room (shown in Figure 34).

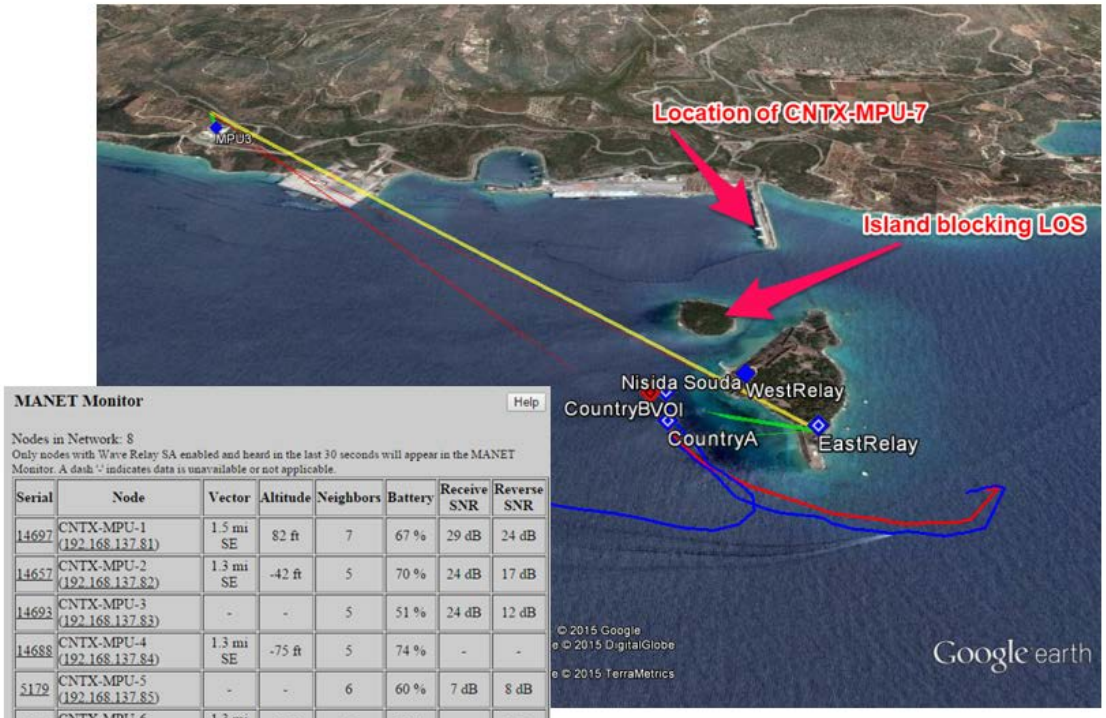
Figure 34. CENETIX Resource Portal VC1 Tool in Use during June 2015 Experiment

This experiment was limited to several small patrol boats, so the scale of the experiment was manageable. However, it was apparent that network management limitations would have a tremendous impact as the scale and complexity of the network increased with the number of nodes and types of networked assets in future experiments.

A key enabler for NOC personnel to identify and mitigate issues caused by cyber and physical clutter were the 3-D visualization tools available through the SA Server and the Wave Relay KML. In this case, the presence of terrain (Nisida Souda Island) impeded LOS communications between two groups of distributed nodes. The use of Google Earth, combined with the Wave Relay KML overlay, gave NOC personnel the ability to correlate the connectivity loss to the presence of physical clutter and obstructions that created interference. The 3-D visualization subsequently gave network operators the ability to optimize the placement of a network relay node and provided immediate feedback based on the network topology reconfiguration. In this case, the feedback was based on the NOC's view of the "MANET Monitor" tab of the Wave Relay Management Interface (Figure 35). This image was taken when the patrol boats from Country A and B

were ordered by the NOC to intercept the target vessel. This view of the Management Interface informed NOC personnel that connectivity had been lost with CNTX-MPU-7 (the MPU-4 radio assigned the boarding team aboard ex-Aris).

Figure 35. MANET Monitor and Map View during Patrol Boat Maneuver in Souda Bay, Crete



MANET Monitor Help

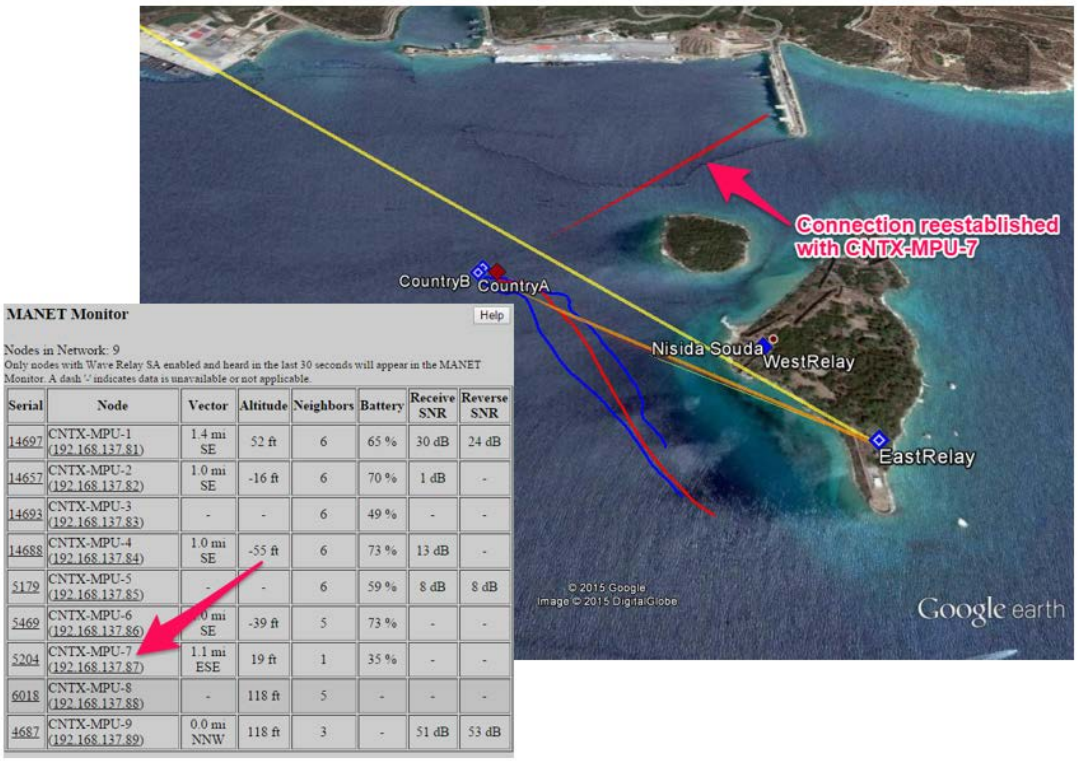
Nodes in Network: 8

Only nodes with Wave Relay SA enabled and heard in the last 30 seconds will appear in the MANET Monitor. A dash '-' indicates data is unavailable or not applicable.

Serial	Node	Vector	Altitude	Neighbors	Battery	Receive SNR	Reverse SNR
14697	CNTX-MPU-1 (192.168.137.81)	1.5 mi SE	82 ft	7	67 %	29 dB	24 dB
14657	CNTX-MPU-2 (192.168.137.82)	1.3 mi SE	-42 ft	5	70 %	24 dB	17 dB
14693	CNTX-MPU-3 (192.168.137.83)	-	-	5	51 %	24 dB	12 dB
14688	CNTX-MPU-4 (192.168.137.84)	1.3 mi SE	-75 ft	5	74 %	-	-
5179	CNTX-MPU-5 (192.168.137.85)	-	-	6	60 %	7 dB	8 dB
5469	CNTX-MPU-6 (192.168.137.86)	1.3 mi SE	-52 ft	5	73 %	-	1 dB
6018	CNTX-MPU-8 (192.168.137.88)	-	242 ft	5	-	-	-
4687	CNTX-MPU-9 (192.168.137.89)	0.1 mi SSE	101 ft	4	-	52 dB	51 dB

Country A and Country B vessels were directed to continue their interception and boarding of the target vessel. As the patrol vessels moved out of the blockage zone caused by the island, NOC personnel were able to see the rediscovery of CNTX-MPU-7 (depicted in Figure 36).

Figure 36. Rediscovery of CNTX-MPU-7 Visible in Wave Relay Management Interface



The Wave Relay Management Interface does not store network performance information so there was no manufacturer-provided solution to view track history via Google Earth 3D visualization. Using the CENETIX SA server, NOC personnel were able to view track history and replay this information for analysis. The ability to view and replay track history enabled network operators to better localize and correlate the causes of network performance fluctuations as part of post-mission or post-failure analysis.

The integration of unmanned systems during the June 2015 experiment significantly contributed to the concepts put forth in this thesis. Unfortunately, UAV mechanical issues after the first flight prevented in-depth testing during the field experiment. The implications of aerial relay nodes are well known (as discussed in Chapter II), but initial experiment results point to the immense potential benefit for network operators to have a real-time view of the impact of UAV mobility within

dynamic MANET topologies. Additionally, the concept of using UGVs as network relays has merit. The ability to leverage terrain features to provide a semi-fixed network relay position enables the use of more robust equipment because UGVs do not have the same weight capacity limitations as UAVs. During this experiment, the ability to view the UGV node's location via network visualization provided network operators the means to identify inadequate node placement and direct movement to optimize network performance.

B. CENETIX COUNTER-WMD EXPERIMENT (OCTOBER 2015) OBSERVATIONS

Building on the knowledge gained in the June 2015 experiment, CWMD experimentation in October 2015 continued to explore distributed knowledge sharing, leveraging a centralized location for operational C2 and network management located at the USCG Station Yerba Buena in San Francisco Bay. As discussed in Chapter III, a primary focus of this experiment was the use of distributed assets across the CENETIX backbone network, including unmanned ground and underwater vehicles. This section outlines the observations and conclusions based on the October 2015 CWMD experiment.

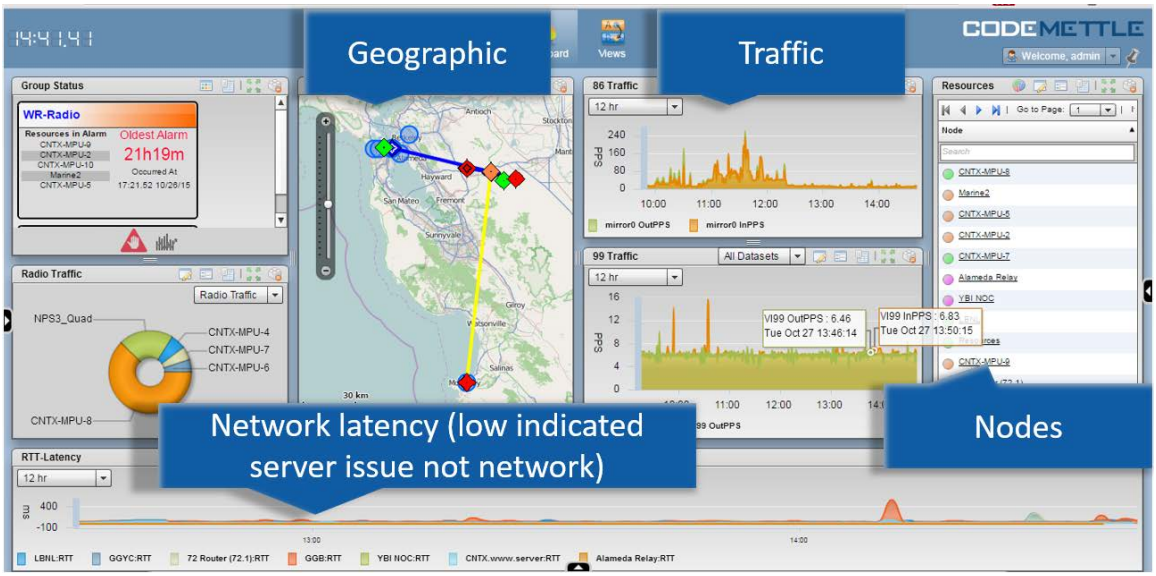
The distributed and hybrid nature of the experimentation network exceeded the capabilities of the Wave Relay Network Management tool. The open-architecture design of the CodeMettle system filled this gap by integrating inputs from traditional network management information protocols (e.g., SNMP), as well as MANET node/network data previously available through the Wave Relay Management Interface.

The unified network dashboard provided network operators direct access to critical network management functionality. CodeMettle allowed users to see performance, configuration and fault information without having to sort through multiple windows or tabs. The integrated map provided a holistic view of the network, including the ability to quickly identify clutter and direct the movement of nodes to compensate for fluctuations in network performance or changes in mission requirements. Additionally, the rich graphical representation of node and network QoS information reduced

equivocality for network operators. This evolution from textual display of network performance data to a graphical illustration of this information combined with map view of node location and links, reduced ambiguity in interpreting network changes and improved the network operator's ability to quickly gain situational awareness.

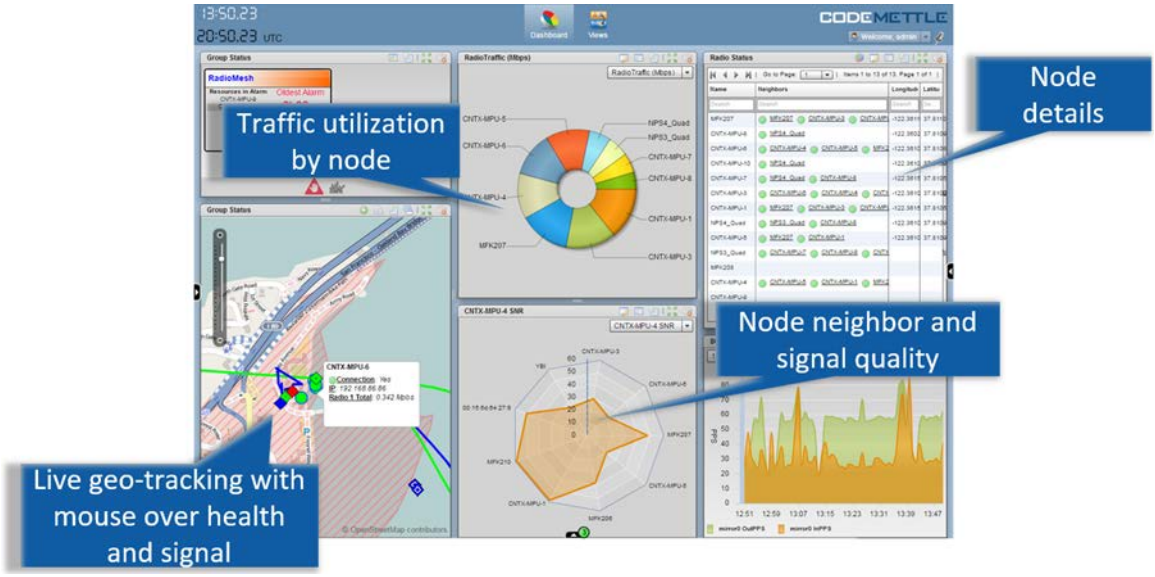
Arguably, one of the most significant observations regarding the use of CodeMettle was the emergence of pattern recognition-enabled network management responses. The CENETIX testbed network experienced several major faults that temporarily halted the experiment; several of these faults would not have been visible if investigators had been solely relying on the Wave Relay Management Interface. For example, during the first day of experimentation researchers found that they were unable to access collaborative tools on the CENETIX Resource Portal. It was initially assumed by researchers in the field that there was a severed communications link within the CENETIX backbone network. However, the CodeMettle interface provided a clear indication to network operators that the low latency within the network pointed to a server issue, not a degraded communication link within the network. Figure 37 depicts the NSO dashboard view fault as the fault occurred. Using this information, CENETIX personnel were able to resolve the server malfunction quickly and the experiment continued.

Figure 37. CodeMettle NSO Dashboard View during Major Server Fault



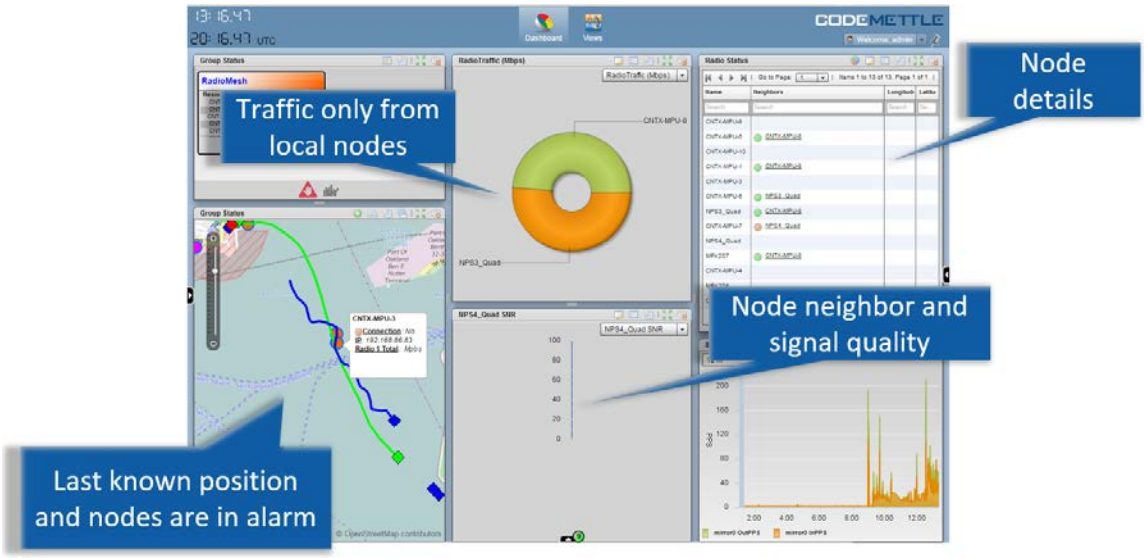
A similar observation occurred during the second day of experimentation in San Francisco Bay. During this phase of the experiment, six U.S. Coast Guard Auxiliary boats and a San Francisco Police maritime patrol vessel were equipped with MANET radios and were tasked to intercept a target vessel. Figure 38 shows these nodes operating normally immediately after getting underway from Yerba Buena Island.

Figure 38. Normal MANET Operations during October 2015 Experiment



After the boats were underway and moving to intercept the target vessel, the NOC consistently lost the ability to communicate with them at a range of approximately 4 kilometers from Yerba Buena Island. Using the CodeMettle NSO Tactical Dashboard, network operators quickly recognized that they were still able to connect with two Wave Relay radios that were within the NOC but could not connect with the MPU-4s on the boats. Figure 39 shows the dashboard view during this fault. This immediately indicated that the connection between the Wave Relay Quad Radio router's sector antenna located on the tower adjacent to the NOC building was no longer functioning correctly. There was no fault indication provided to the network operator because CodeMettle could not directly communicate with the Wave Relay Quad Radio router located on the tower due to the configuration of the USCG network firewall. However, the network operator did receive fault indications due to the loss of communications with the underway nodes. It was subsequently determined that the boats were initially communicating directly to the radios in the NOC building and that the Quad Radio router

Figure 39. Quad Radio Failure as Viewed from CodeMettle NSO



Overall experimentation required a hybrid approach to backbone networking due to resource limitations and operational constraints (e.g., access to multiple UAVs and airspace restrictions preventing UAV operations in San Francisco Bay). Coupled with the distributed nature of experiments over a wide geographic area, the October 2015 experiment required the use of satellite communication systems—satellite connectivity was required to network UGV inland and remote UUV connection. The inability to rely solely on MANET communications for this experiment points to the challenge of ensuring adequate node density to support mission requirements. This also indicates the relevance and potential contributions of tactical cube and pico-satellites in littoral operations.

The integration of unmanned vehicles during the October 2015 experiment yielded observations very relevant to littoral operations. For example, even though UUV operations are still nascent, NUWC Keyport has devoted significant resources to the research and development of new UUV technologies and C2 capabilities required to make them viable for tactical operations. There is significant potential tactical benefit for the use of UUVs as networked nodes to provide undersea surveillance as well as to contribute covert site exploitation information for tactical operations. Information provided by UUV nodes would contribute to the commander's understanding of the

environment and potentially provide covert means to share information across a hostile environment. Additionally, the use of UGVs in littoral areas, both as network relays and sensing platforms, allows littoral commanders to extend their influence and capabilities ashore while reducing risk to personnel in dangerous environments. This is particularly relevant in the realm of counter-WMD and the stand-off detection of radiological/nuclear materials.

C. LITTORAL OPERATIONS VIGNETTE

Consider the littoral operations scenario offered in Chapter I—an AFP tasked to conduct EMIO operations in a contested littoral environment. UAVs are launched to search a near-shore region for an unmarked FIAC carrying a container of nuclear material; their effective search area is expanded by their ability to relay telemetry and sensor data to UAVs operating past LOS range of the AFP. The network operator sees not only the PLI for the UAV, but also the health of the links between the UAVs and can direct their positioning to ensure the network connection is maintained for the mission-critical video feed coming from the UAV. After identifying the potential target vessel, the AFP launches a USV carrying a standoff nuclear detection system. The USV is tasked to conduct standoff detection to confirm the identity of the vessel, however the target vessel moved behind a small island. It is not clear to the network operator if the island will block communications between the USV and AFP. As the USV navigates around the island, network connectivity between the USV and the AFP becomes degraded; the network operator subsequently restores this connection by choosing a UAV to maneuver in order to extend the overhead relay link to the USV. The USV detects the presence of the radioactive isotope and transmits the spectrograph back to the AFP for reachback analysis. Once confirmed, two Mark VI patrol boats are directed to intercept and board the vessel. As they close the VOI, the network operator detects failing node links, and then receives fault notifications in the NMS indicating a potential jamming source from the adjacent shoreline. In response, the network operator directs the movement of one UAV a closer location to attempt to burn through the attempted jamming and restore the communications link to the patrol boat. Initial indications showed that this was insufficient, so the network operator maneuvers the UAV and USV in tandem to bolster

the network connection with the patrol boat by chaining the relay nodes and leveraging the higher transmit power of the USV to overcome the jamming signal.

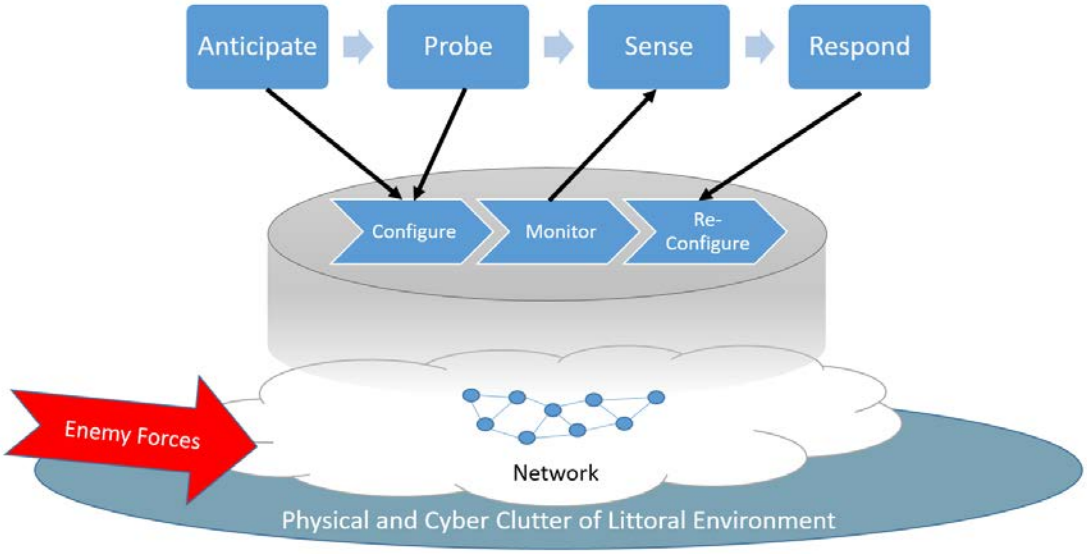
During this hypothetical scenario, the decision-maker was faced with providing all functions of MANET management (configure, heal, optimize, monitor and protect). The effects of these functions in cyberspace manifest in the physical realm. As a result, the robustness and adaptability of this network were enabled by MANET node mobility as a function of network configuration and reconfiguration. Based on the observations and findings of CENETIX experimentation, this is most effectively accomplished through a unified network management approach. More specifically, the combination of graphically-represented network performance information and 3-D map visualization of networked nodes would provide the network operator the ability to maintain situational awareness and more effectively direct the placement of these nodes.

The complex domain of the littorals precludes the ability for a decision-maker to be fully aware of what impacts the combination of environmental dynamics, enemy action and the movements of their own assets will have on their network. However, as discussed in Chapter II, the decision maker can anticipate initial conditions, to some degree, based on a preconceived understanding of the mission, tacit knowledge gained from previous experiences, and initial or intended friendly force disposition. The use of MANET in the littorals expanded decision maker's ability to observe patterns of response through networked UAV and USV nodes. These nodes also provided multiple "safe-to-fail" options, allowing the network operator to probe network performance changes using topology manipulation (e.g., the ability to move several different nodes to bolster the network connection to the patrol boat). The network operator was able to observe the effects of the first node movement to determine if the actions were successful. When initial observations indicated different results than expected, the network operator had the flexibility to adjust and adapt to the situation.

By breaking down the process elements from the decision-making and network management perspectives, it is possible to map them as they interact with each other as well as through the network that is impacted by cyber and physical clutter and enemy

action. The model depicted in Figure 40 does not directly consider the enemy's decision process; rather, it addresses enemy activity as a direct influencer on the physical network.

Figure 40. Cyber-Physical Network Decision-making Model



In this model, anticipatory and probing actions previously discussed directly influence the configuration of the MANET as it is deployed. Patterns of response to probing actions are sensed through the monitoring functions of network management. Response actions result in reconfiguration that contribute to the robustness and adaptation of the MANET to counter the effects of cyber and physical clutter.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CONCLUSIONS AND RECOMMENDATIONS

The objective of this thesis has been the exploration of emerging network management tools as they support tactical-level mesh networks and their impact on C2 decision making in the littoral domain. A specific contribution of this research was the demonstration of the value of network management tools for the human-network interface and, by reducing uncertainty and equivocality, the positive impact of effective network management on situational awareness and decision making in the littorals. Emerging network management tools can support tactical-level MANET and influence C2 in littoral operations by providing decision makers (e.g., the Tactical Action Officer) real-time awareness of dynamic MANET topology and the ability to effectively redirect and reposition networked assets to mitigate network performance fluctuations and support mission requirements.

Cyber-physical systems embody the integration of computational and physical capabilities that enable interaction with the physical world across cyber space; understanding, visualizing, and managing this interaction through the human-network interface is a crucial step forward towards integrating manned and unmanned systems in the complex littoral environment. The unique nature of the littoral environment, in terms of the presence of physical and cyber clutter discussed earlier, makes the importance of physical layer management even more relevant. The integration of manned and unmanned platforms will require a paradigm shift in how a force's actions affect, and are impacted by, the dynamic nature of physical and cyber clutter within the littoral battlespace.

A. CONCLUSIONS

Throughout this thesis, discussions regarding network management have relied on abstractions as a means to simplify immensely technical processes and technologies. In reality, network operators are not dealing with abstract nodes—network management and network adaptation occurs at all layers of the OSI stack. For example, "healing" mechanisms may refer to elements at the internet layer (e.g., resilient proactive/reactive

routing protocols) but can also apply to the application layer. Likewise, protection plays an important role at all layers within the network (e.g., intrusion detection, firewalls, encryption, etc.). These inner workings of network management functionality are critical to the operation of any network, tactical or otherwise. However, traditional network management functions are, and in many ways should be, transparent to the commander making decisions in a tactical environment unless some aspect of the network is compromised or fails to work as designed. In contrast, MANET physical layer management must be explicitly considered during mission planning and asset deployment to be effective. Therefore, the critical convergence between MANET management and C2 decision-making in the littorals occurs at the OSI physical layer via topology control and the physical placement and maneuver of network nodes.

The complexity of the littorals, and the previously discussed implications on MANET management in the littoral domain, warrant consideration that the tactical-level decision maker becomes a network operator, who directly interprets human-network interface information to determine overall network effectiveness and direct action in order to fight the network (and sensors) as a weapons system. The network agnostic approach used by CodeMettle for the management of heterogeneous networked systems, standards and protocols provides a new level of flexibility to give network operators a holistic view of the network. As conventional network management systems are not compatible with MANET technologies, the open-architecture design of the CodeMettle software allows the integration of inputs from traditional network management information protocols (e.g. SNMP), as well as MANET node/network data previously available through the Wave Relay Management Interface and Wave Relay API. The unified network management approach enables the network operator to perceive and proactively manipulate the network.

Human perception drives the creation of knowledge, awareness and understanding, resulting in action through decision-making in the cognitive domain. The complex decision domain faced in the littorals requires decision makers to identify multiple courses of action and maintain them as probing actions can reveal emergent order from patterns of response within the network. Because the response patterns may be

subtle and manifest over time, or be interpreted in different ways, perceiving these responses requires a rich human-network interface visualization. Improving decision-making cycles requires real-time situational understanding of the scalable and flexible mesh architecture in littoral operations. Mobile ad hoc networks require constant reconfiguration based on network performance feedback. Data from the entire network must be collected and viewable by network operators in order to take advantage of the dynamic topologies of mesh networks through node mobility. The opportunity to explore CodeMettle's unified dashboard interface during the October 2015 experiment indicated that the network operator's ability to quickly identify, assess, and react to changes in network performance was greatly enhanced when compared to the textual display in the Wave Relay Management Interface.

The US Navy currently lacks the ability to efficiently anticipate or redirect assets in response to network degradation resulting from interactions with physical and cyber clutter unique to the littorals. During June 2015 CENETIX experimentation, map visualization was a key enabler for NOC personnel to identify and mitigate issues caused by cyber and physical clutter. Additionally, map visualization gave network operators the ability to optimize the placement of network relay nodes and provided immediate performance feedback based on the network topology reconfiguration. The 2D map interface available in the October 2015 iteration of the CodeMettle NSO developed for CENETIX performed adequately when compared to the 3D KML available from the CENETIX SA Server and Wave Relay Management Interface. However, UAV operations were not included in the October 2015 experimentation. The benefits of 3D visualization for UAV operations during June 2015 experimentation were apparent and the development of 3D maps for the CodeMettle dashboard has been recommended to the CodeMettle team.

MANET technology is the manifestation of NCW at the tactical edge. However, the implementation of multi-hop mesh networking capabilities to provide adaptive and resilient networking in support of collaboration and C2 in high-density, complex or contested environments at the tactical edge requires an aggressive approach to network management. Modern U.S. littoral warfare can capitalize on the integration of a new

generation of vessels, such as the Littoral Combat Ship (LCS), by applying MANET technologies to enable shared data flows between other littoral assets and unmanned systems and sensors functioning as network nodes. The combination of these assets will be enabled through a self-forming, self-healing mesh network that improves information sharing, increasing situational awareness and overall mission effectiveness in the littorals and beyond. However, the full-scale integration of tactical maritime UxV systems is codependent with ubiquitous MANET implementation. Additionally, the human-network interface supporting the tactical management of these networks must be a primary consideration in order to maximize the potential benefits of these technologies in the complex littorals.

B. FUTURE WORK

This thesis builds upon ongoing CENETIX research and experimentation campaigns to further the operationalization of network management; however, it does so with an emphasis on implications for network management as a warfighting tool in the littoral domain. As an exploratory thesis, some of the conclusions herein represent nascent hypotheses that would benefit from quantitative testing. Other assertions in this thesis challenge traditional organizational/doctrinal paradigms and require in-depth analysis.

The human-network interface as the primary conduit for building human perception to create knowledge, and subsequently drive action in the cognitive domain, is an area that requires further consideration. The emergence of pattern recognition behavior with network visualization tools as an enhancement to traditional network management methods may provide avenues for improving response time and sensitivity to network performance degradations. A quantitative hypothesis based on this observation may yield useful insights into how future tactical network management systems should address human-systems integration issues.

From an organizational standpoint, the implications of role-based relationships and the flattening of organizational structures in MANET-enabled, small-unit groups for the culture and doctrine of the U.S. Navy need to be analyzed, specifically, the

relationship between the AFP, traditional hierarchical command structures, and the CWC construct for maritime C2. With regards to managing the network as a weapons system, a robust concept of operations is required to identify roles, responsibilities, capabilities and information requirements at each level of command (e.g., ship, AFP, Task Force).

The primary assumption of this thesis is that the U.S. Navy will continue to move forward with the development of MANET systems. However, the implementation of MANET technology and management systems still face tremendous technical challenges before these systems can be fielded in the tactical maritime environment. This will require further research and development for MANET systems at every level of the OSI stack. Furthermore, continued research into integrating commercial-off-the-shelf MANET systems for UxV control and relay capability for tactical operations in the littorals can provide crucial insights for the design and production of new UxVs that are integrate with next generation MANET systems (including "smart" physical layer capabilities, like phased array antennas, to improve radio performance and lower probability of interception/detection). Physical layer implementation research could also benefit from further exploration into the use of control links (separate from data link connections) to provide an out-of-band mesh control layer to improve manageability of highly dynamic MANET. Additionally, the application and management of delay-tolerant networks as a means to provide resilient data paths in disconnected, intermittent, or low-bandwidth environments should be considered.

The dynamic management of MANET-enabled assets will require the incorporation of UxV control, C2 and network management functions into a unified system. The open-architecture design of new network management systems like CodeMettle provide significant flexibility and adaptability to evolve with improvements in technologies and capabilities. However, the ability to connect and integrate these systems with shipboard networks requires further investigation.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Alberts, D. S. (2002). *Code of best practice: Experimentation*. Washington, DC: DOD Command and Control Research Program.

Alberts, D. S., Garstka, J. J., Hayes, R. E., & Signori, D. A. (2001). *Understanding information age warfare*. Washington, DC: DOD Command and Control Research Program.

Baheti, R., & Gill, H. (2011). Cyber-physical systems. *The Impact of Control Technology*, *12*, 161–166.

Bar-Yam, Y. (2003). *Complexity of military conflict: Multiscale complex systems analysis of littoral warfare*. Cambridge, MA: New England Complex Systems Institute. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.132.6248&rep=rep1&type=pdf

Bauer, B., & Patrick, A. S. (2004). A human factors extension to the seven-layer OSI reference model. Retrieved from http://www.andrewpatrick.ca/OSI/10layer.html

Bergin, R., Hudgens, B., & Nissen, M. (2011). Examining work performance in immersive virtual environments versus face-to-face physical environments through laboratory experimentation. In *Proceedings of the 44th Hawaii International Conference on System Sciences (HICSS)*, 1–10.

Bordetsky, A., Benson, S. J., & Hughes, W. P. (n.d.). (in press). Mesh networks in littoral ops.

Bordetsky, A., & Hayes-Roth, R. (2006). Hyper-nodes for emerging command and control networks: The 8th layer. In *Proceedings of 11th International Command and Control Research and Technology Symposium*. Retrieved from http://www.dodccrp.org/events/11th_ICCRTS/html/papers/127.pdf

Bordetsky, A., & Netzer, D. (2010). Testbed for tactical networking and collaboration. *The International C2 Journal*, *4*(3). Retrieved from http://www.dodccrp.org/files/IC2J_v4n3_B_Bordetsky.pdf

Butler, A. (2012). U.S. Marine Corps explores extended-range blackjack. Retrieved from http://aviationweek.com/defense/us-marine-corps-explores-extended-range-blackjack

Cares, J. R. (2005). *Distributed networked operations: The foundations of network centric warfare*. Newport, RI: Alidade Press.

Cebrowski, A. K., & Garstka., J. J. (1998). Network-centric warfare : Its origin and future. In *US Naval Institute Proceedings*, (January), 28–35.

Chan, S. (2001). Complex adaptive systems. In *ESD.83 Research Seminar in Engineering Systems*, 1–9. http://doi.org/10.1002/cplx.20316

Chun, I., Park, J., Kim, W., Kang, W., Lee, H., & Park, S. (2010). Autonomic computing technologies for cyber-physical systems. *The 12th International Conference on Advanced Communication Technology (ICACT)*.

Clemm, A. (2006). Network management fundamentals. Retrieved January 12, 2016, from http://techbus.safaribooksonline.com/book/networking/network-management/1587201372

Cognitive Edge. (n.d.). The cynefin framework [video]. Retrieved February 23, 2016, from https://www.cognitive-edge.com

Daft, R. L., & Lengel, R. H. (1986). Organizational information requirements, media richness and structural design. *Management Science*, *32*(5), 554–571.

Department of the Navy. (2015). A cooperative strategy for the 21st century seapower. Washington, DC: Author.

Dolgov, I., & Hottman, S. (2012a). Challenges in unmanned aircraft systems. In R. Barnhart, S. Hottman, D. Marshall, & E. Shappee (Eds.), *Introduction to Unmanned Aircraft Systems* (1st ed., pp. 165–180). Boca Raton, FL: CRC Press.

Dolgov, I., & Hottman, S. (2012b). Challenges in Unmanned Aircraft Systems. In R. Barnhart, S. Hottman, D. Marshall, & E. Shappee (Eds.), *Introduction to Unmanned Aircraft Systems* (1st ed., pp. 165–180). Boca Raton: CRC Press.

Everly, R., & Limmer, D. (2014). *Cost-effectiveness analysis of aerial platforms and suitable communication payloads*. Master's thesis, Naval Postgraduate School, Monterey, CA.

Fama, E. F., & Jensen, M. C. (1983). Separation of ownership and control. *The Journal of Law & Economics*, *26*(2), 301–325.

Frye, L., & Cheng, L. (2010). A network management system for a heterogeneous, multi-tier network. In *GLOBECOM - IEEE Global Telecommunications Conference*, 1–5. http://doi.org/10.1109/GLOCOM.2010.5683112

Gateau, J. (2007). *Extending simple network management protocol (SNMP) beyond network management: a MIB architecture for network-centric services*. Master's thesis, Naval Postgraduate School, Monterey, CA.

Grant, T., & Kooter, B. (2005). Comparing OODA & other models as operational view C2 architecture. In *Proceedings of the 10th International Command and Control Research Technology Symposium*.

Haider, Z., & Shabbir, F. (2014). Genetic based approach for optimized routing in maritime tactical MANETs. In *11th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, doi: 10.1109/IBCAST.2014.6778194

Hughes, W. P. (2000). *Fleet tactics and coastal combat* (2nd ed.). Annapolis, MD: Naval Institute Press.

International Organization for Standardization (ISO). (1996). Information technology - Open systems interconnection - Basic reference model: The basic model. *International Standard ISO/IEC 7498-1*. Retrieved from http://standards.iso.org/ittf/PubliclyAvailableStandards/s025022_ISO_IEC_7498-3_1997(E).zip

Joint Chiefs of Staff. (2011). *Joint Interdiction* (Joint Publication 3-03). Washington DC: U.S. Government Printing Office.

Joint Chiefs of Staff. (2015a). *Department of Defense dictionary of military and associated terms (*Joint Publication 1-02). Washington, DC: U.S. Government Printing Office.

Joint Chiefs of Staff. (2015b). *Joint communication system* (Joint Publication 6-0). Washington, DC: U.S. Government Printing Office.

Joint Chiefs of Staff. (2015c). *Joint concept for command and control of the Joint Aerial Layer Network*. Washington, DC: U.S. Government Printing Office.

Kidston, D., & Kunz, T. (2008). Challenges and opportunities in managing maritime networks. *Communications Magazine, IEEE, 46*(10), 162–168. doi: 10.1109/MCOM.2008.4644135

Koch, R., & Golling, M. (2015). Blackout and now? Network centric warfare in an anti-access area-denial theatre. In *Proceedings of 7th International Conference on Cyber Conflict: Architectures in Cyberspace (CyCon)*, 169–184.

Lindberg, M., & Todd, D. (2001). *Brown-, green-, and blue-water fleets : The influence of geography on naval warfare, 1861 to the present*. Westport, CT: Praeger.

Liu, Z., Yang, D., Wen, D., Zhang, W., & Mao, W. (2011). Cyber-physical-social systems for command and control. *IEEE Intelligent Systems*, (4), 92–96.

Misra, S. C., Misra, S., & Woungang, I. (Eds.). (2009). *Guide to wireless mesh networks*. London, England: Springer. Retrieved from http://libproxy.nps.edu/login?url= http://link.springer.com/book/10.1007/978-1-84800-909-7/page/1

National Defense Research Institute. (2013). *U.S. Navy employment options for unmanned surface vehicles (USVs)*. Santa Monica, CA: RAND.

Naval Postgraduate School. (n.d.). About The Littoral Operations Center. Retrieved January 11, 2016, from http://www.nps.edu/Academics/Schools/GSOIS/Departments/DA/LOC/LOC_About.html

Network Management Reference Architecture. (2008). Retrieved February 12, 2016, from http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white_paper_c11-453503.html

Pathmasuntharam, J. S., Kong, P. Y., Zhou, M. T., Ge, Y., Wang, H., Ang, C. W., … Harada, H. (2008). TRITON: High speed maritime mesh networks. In *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*. doi: 10.1109/PIMRC.2008.4699972

Peacock, B. (2007). *Connecting the edge: Mobile ad-hoc networks (MANETs) for network centric warfare. Blue Horizons*. Air War College. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA497761

Pfeffer, J., & Salancik, G. R. (2003). *The external control of organizations: A resource dependence perspective*. Stanford, CA: Stanford University Press.

Puff, C. J. (2011). *Network management system for tactical mobile ad hoc network segments*. Master's thesis, Naval Postgraduate School, Monterey, CA.

Quincy, K. E., Johnson, J. J., Moran, M. G., Nilsson, D. J., & Thompson, B. G. (2010). *An integrated command and control architecture concept for unmanned systems in the year 2030*. Master's thesis, Naval Postgraduate School, Monterey, CA.

Radiocommunication Sector of International Telecommunication Union. (2011). *Maritime broadband wireless mesh networks* (Vol. M.2202). Geneva, Switzerland.

Ren, J., & Li, T. (n.d.). Network Management.

Richard, M. (2009). *Cooperative control of distributed autonomous systems with applications to wireless sensor networks*. Master's thesis, Naval Postgraduate School, Monterey, CA.

Rothal, J., Davis, A., & Marlatt, G. E. (2015). *A sampling of NPS theses, reports and papers on UxS*. Monterey, CA: Naval Postgraduate School.

Rowden, T., Gumataotao, P., & Fanta, P. (2015). "Distributed Lethality." *Proceedings, 141*(1). Retrieved from http://www.usni.org/magazines/proceedings/2015-01/distributed-lethality

Shenoy, N. (n.d.). Network management - Introduction. Rochester Institute of Technology.

Shim, J. P., Warkentin, M., Courtney, J. F., Power, D. J., Sharda, R., & Carlsson, C. (2002). Past, present, and future of decision support technology. *Decision Support Systems*, *33*(2), 111–126.

Sichitiu, M. (2006). *Journey from Mobile Ad Hoc Networks to Wireless Mesh Networks*. *Ad Hoc Networks*. Raleigh, NC: North Carolina State University.

Snowden, D. J. (2012). The OODA loop & cynefin. Retrieved February 23, 2016, from http://cognitive-edge.com/blog/the-ooda-loop-cynefin/

Snowden, D. J., & Boone, M. E. (n.d.). A leader's framework for decision making. *Harvard Business Review November 2007*, *85*(11), 68. Retrieved from https://hbr.org/2007/11/a-leaders-framework-for-decision-making

Solomon, J. (2015). Information dissemination: Distributed lethality is about far more than just ships shooting ships. Retrieved from http://www.informationdissemination.net/2015/07/distributed-lethality-is-about-far-more.html

Subramanian, M. (2010). Network management: principles and practice. Pearson Education India. Retrieved from http://techbus.safaribooksonline.com/book/networking/network-management/9788131727591

Sweeney, M. M. (2002). *An introduction to command and control*. Master's thesis, Naval Postgraduate School, Monterey, CA.

Team CASA. (2014). *Disruption-tolerant networking and computing*.

U.S. Department of Defense. (2013). Unmanned systems integrated roadmap 2013 - 2038. Washington, DC: Author.

Van Creveld, M. L. (1985). *Command in war*. Cambridge, MA: Harvard University Press.

Vego, M. (2015). On littoral warfare. *Naval War College Review*, *68*(2), 30–68.

Wade, J. F. G. (1996). *Navy tactics, doctrine, and training requirements for littoral warfare*. Master's thesis, Naval Postgraduate School, Monterey, CA.

Ya'ari, Y. (2014). The Littoral Arena: A word of caution. *Naval War College Review*, *67*(3), 7–21.

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