2004-12

Designing a FORCEnet information topology

Krajacich, Christopher A.

Monterey California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DESIGNING A FORCENET INFORMATION TOPOLOGY

by

Christopher A. Krajacich

December 2004

Thesis Advisor: Dan Boger
Thesis Co-Advisor: William Kemple

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** December 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Designing a Forcenet Information Topology			**5. FUNDING NUMBERS**
6. AUTHOR(S) Krajacich, Christopher A.			
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.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Network Centric Warfare (NCW) is a theory of war that attempts to maximize the benefit of linking together, or networking, operating forces. The Navy and Marine Corps have decided to attempt to instantiate this warfighting concept through FORCEnet. The FORCEnet concept is ambitious, but most current efforts have looked to ensure the ability to connect and share data without addressing the larger picture of how to move information within a netted force in order to maximize the benefit of information sharing. This thesis presents an information topology developed to effectively share information across a variety of force compositions. In order to fully attain the benefits of a networked force, a complementary command and control system must also be designed. This thesis also outlines a command and control system that can be employed in a network-centric force.

14. SUBJECT TERMS Network Centric Warfare, NCW, Net-Centric Operations, FORCEnet, Information Topology			**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** UL

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.

DESIGNING A FORCENET INFORMATION TOPOLOGY

Christopher A. Krajacich
Captain, United States Marine Corps
B.S., Virginia Polytechnic Institute, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
December 2004

Author: Christopher A. Krajacich

Approved by: Dan Boger
Thesis Advisor

William Kemple
Co-Advisor

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Network Centric Warfare (NCW) is a theory of war that attempts to maximize the benefit of linking together, or networking, operating forces. The Navy and Marine Corps have decided to attempt to instantiate this warfighting concept through FORCEnet. The FORCEnet concept is ambitious, but most current efforts have looked to ensure the ability to connect and share data without addressing the larger picture of how to move information within a netted force in order to maximize the benefit of information sharing. This thesis presents an information topology developed to effectively share information across a variety of force compositions. In order to fully attain the benefits of a networked force, a complementary command and control system must also be designed. This thesis also outlines a command and control system that can be employed in a network-centric force.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. AREA OF RESEARCH

The purpose of this research is to design an information topology for FORCEnet that delivers information to a Decision Maker in order to gain a Decision Making Advantage. In addition, this paper will identify some gaps in current technologies and emerging technologies that may fill those gaps. In addition, this thesis will show how the proposed information topology will support Network Centric Warfare principles and how it would be employed.

B. RESEARCH QUESTIONS

How should FORCEnet be organized so that information can flow effectively and efficiently and be delivered to the right person at the right time in the right format? What command and control structure or decision making organization will best capitalize on the FORCEnet information structure to ensure that warfighting capabilities are enhanced?

C. BACKGROUND

1. General

As part of Sea Power 21, the US Navy has decided to move toward Network Centric Warfare as its future war fighting concept. The concept is based on the idea of rapid information sharing via robust communications, and draws it power from the ability to link together, or network, a military force.[1] The concept of self-synchronization of forces was the major principle on how to

[1]David S. Alberts, John J. Gartska, and Frederick P. Stein, *Network Centric Warfare*. (Washington: Department of Defense, 1999), 93-94.

change the way a Net-Centric force would fight[2], but later works have added the idea of swarming[3] which has gained popularity in the last few years.

a. Self-synchronization

Self-synchronization is founded on the concept that empowered units with the same view of the battlespace and the same understanding of the commander's intent can laterally coordinate and prosecute the battle with minimal input from higher command levels[4]. This idea is not entirely new, and examples include the German army of World War II who used a similar concept of mission orders and commander's intent to allow their units to quickly and decisively fight. Also, the US Marines have adopted a similar concept in their Maneuver Warfare Doctrine. The goal of self-synchronization is that small, independent units can act together as a coherent force with "big picture" guidance to achieve common goals. This allows a faster pace of operations because forward units do not need to wait for instructions from higher headquarters, and faster actions on the battlefield will translate into decisive victories. This thesis will look at the possibility of self-synchronization, which hinges on information sharing and the belief that given the same picture of the battlefield, different leaders will come to a common solution.

---

[2] Arthur K. Cebrowski and John J. Gartska, "Network Centric Warfare: Its Origin and Future," *Proceedings of the U.S. Naval Institute,* January 1998

[3] Bruce Berkowitz, *The New Face of War*. (New York: The Free Press, 2003), 100-118

[4]David S. Alberts, John J. Gartska, and Frederick P. Stein, *Network Centric Warfare*. (Washington: Department of Defense, 1999), 175-176.

b. Swarming

Swarming is simply bringing together disparate forces at a decisive place to mass their effects, and then withdrawing them back to a dispersed disposition. Swarming relies heavily on robust, effective communications. Small, disparate forces need to be able to communicate reliably, and often covertly, in order to affect a swarm-like attack. Again, this is not a new concept and is encapsulated in the Marine Maneuver Warfare doctrine in the form of massed fires replacing massed forces, although to a lesser degree than espoused in the principles of Network Centric Warfare. The advantage of using a swarming force is that troops and equipment no longer need to mass for long periods of time in order to achieve combat power. Instead the mass their effects at the decisive point on the battlefield and then disperse so that the enemy does not have a large center of gravity to attack. Modern sensors, targeting, and weapons make massing of troops a very dangerous proposition. It is widely recognized that massed troops and equipment will be targeted and destroyed. The ability to keep forces dispersed aids in concealment of forces, as well as survivability of forces when attacked. Another advantage of swarming that is not commonly discussed is that dispersed forces need not be of the same type. Forces from different services, countries, agencies, or specialties can be quickly brought together to achieve a specific mission then quickly dispersed. These forces are regularly called “ad hoc teams” and are expected to be integral to combat in the future.[5]

[5] Bruce Berkowitz, *The New Face of War*. (New York: The Free Press, 2003), 100-118.

2. FORCEnet

The US Navy has decided to operationalize Network Centric Warfare through a concept known as FORCEnet. Unfortunately, FORCEnet is a concept that is poorly defined and often means different things to different people. Sea Power 21 defines FORCEnet as

> the "glue" that binds together Sea Strike, Sea Shield, and Sea Basing. It is the operational construct and architectural framework for naval warfare in the information age, integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force.[6]

Although this definition is fairly clear and breaks out the potential power of FORCEnet (as evidenced by the Army's definition of LANDWARNET which is nearly identical[7]), it does not spell out how FORCEnet will be developed or employed. Nor does it address how FORCEnet will facilitate Network Centric Warfare. So what does FORCEnet really do for us? How does it improve the way we fight as naval services? Should it be separate from the Army and Air Force equivalents?

The first problem with answering the above questions is that FORCEnet is not a thing. It is not a program, system, or piece of equipment that can be identified. It is a concept for operationalizing Network Centric Warfare. Much of the current work in instantiating FORCEnet at the DOD contractor and Systems Command level involves connectivity, bandwidth, and data fusion concerns. Although these are important elements of building any

[6] Adm. Vern Clark, "Sea Power 21," *Proceedings of the U.S. Naval Institute,* October, 2002

[7] LANDWARNET Brief, Futures Center, Training and Doctrine Command, given February, 2004

computer network, better connectivity and formatted data do not equal Network Centric Warfare by themselves.

Most work in the data integration area has had to do with compatible computing schemes and has largely overlooked analysis problems. Modern sensors and data mining programs can produce overwhelming volumes of data, and analysts and commanders are in danger of being presented with more information than any one human can process. Computer aided analysis and integration tools can help with the data overload problem, but filtering software and procedures may become more important. Simply making more information available will not aid the decision making process. Advances in Human System Integration have helped this problem, but little real progress has been made. The data overload problem will continue to get worse as more information is put into the system.

Lastly, and most importantly, almost no work has been put into the information topology of the network. For example, a sensor field gets a hit; where does it send the information? Why? Who decides? There are many answers to this fundamental question, but they are all based on opinions and not analysis. This paper will add some reasoned analysis to this problem.

Fundamentally, what is FORCEnet, and why do we need it? FORCEnet is, in part, an information structure with the primary purpose of delivering tailored information to the Decision Maker, whoever that may be. The structure must be able to aid Decision Makers at all levels, from the Strategic Commander, to the Marine on the ground who decides whether or not to pull the trigger. To build this type of structure, the Navy and Marine Corps need to look

at how people handle information now, and how they want the system to handle information in the future.

D. ORGANIZATION AND SCOPE OF THESIS

Chapter II covers the current body of literature on Network Centric Warfare, FORCEnet policy, and the state of emerging technologies relevant to FORCEnet. It will serve to set the background for the remaining chapters as well as explain some concepts that exist in the DOD regarding FORCEnet. Chapter III will begin the analysis of information and user requirements that will drive the rest of the thesis. This analysis will include the design of a command and control system and information topology that will maximize the potentials of a fully networked force. Chapter IV will describe how information will move between users in the proposed topology and how this design will work with existing and proposed SOP for employing NCW. Chapter V illustrates how the employment of the proposed topology will work in a combat environment.

Building a coherent FORCEnet is an enormous task that is far beyond the scope of any one thesis. This thesis will limit itself to defining an information topology, presenting a command and control concept, identifying technological shortfalls and potential emerging technologies to solve those problems, and making recommendations for a way forward to field FORCEnet that will enable of Network Centric Warfare. To do this, this thesis will look at changing the way the Navy and Marine Corps configure their command and control systems so that FORCEnet can effectively work with Decision Makers to improve combat operations. Finally some recommendations

for simulations and wargames will be made to ensure that the road ahead will lead to future success.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

A. NETWORK CENTRIC WARFARE

1. Vision

The theory of Network Centric Warfare was first put forward by VADM. Cebrowski and John Gartska in a January 1998 issue of the *Proceedings of the U.S. Naval Institute.* They originally envisioned an information network that any soldier, sailor, airmen, or Marine could plug into and send and receive relevant information. The platforms and personnel would be interchangeable within the networked force and included sensor grids, information grids, and shooter grids. They viewed this capability as a way to fundamentally change how U.S. forces are organized and employed.[8] This concept slowly began to take root in the U.S. Navy, and became official doctrine when Secretary of Defense Donald Rumsfeld wrote it into the Defense Planning Guidance.[9]

Network Centric Warfare has come to be associated with Effects Based Operations, largely because both have roots in network analysis. Effects Based Operations is a theory of warfare that proposes that small, properly targeted actions can have large scale effects. EBO attempts to use nodal analysis to determine a desired outcome and walk backward through a complex network to determine which nodes can be targeted to achieve the desired outcome.[10] Although

[8] Arthur K. Cebrowski and John J. Gartska, "Network Centric Warfare: Its Origin and Future," *Proceedings of the U.S. Naval Institute,* January 1998

[9] Bruce Berkowitz, *The New Face of War.* (New York: The Free Press, 2003), 113.

[10] Edward A. Smith, *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War.* (Washington: The Department of Defense).

EBO and NCW share some common language and grew out of similar field of study, they are fundamentally different theories of warfare that have some overlap but are not dependant on each other. Both theories focus on the relationships between nodes and how parts of networks interact, but apply these relationships in different ways. It is important to recognize that the two theories neither rely upon each other, nor are mutually exclusive. EBO still has some advocates in the DOD, but has recently fallen out of favor with many high ranking officers. Whether EBO can ever be operationalized is a subject of another work, but NCW can be employed with or without EBO.

2. Principles

a. Shared Situational Awareness

One of the driving tenets of Network Centric Warfare is Shared Situational Awareness. Situational Awareness (SA) is a detailed understanding of one's environment. On the battlefield, this includes knowledge of not only friendly and enemy dispositions, but plans, contingencies, and Commander's Intent. NCW asserts that if all personnel have a shared view of the battle space, they can achieve Shared Situational Awareness. Advocates of NCW assert that commonly trained units with Shared Situation Awareness should be able to self-synchronize and come to a common course of action. This assertion and self-synchronization are explored in more detail below.

b. Migration of Control

Shared Situational Awareness allows commanders closest to the action to have a complete picture and take action in a rapid manner. To achieve and maintain a fast tempo of operations, it is important to allow forward commanders the freedom to take action at their discretion.

This process is known as migration of control or delegation of authority. Control of forces will migrate from the higher echelons of command to units at the edge of battle. Migration of control, unlike traditional delegation of authority, allows the control of forces to shift laterally from units at similar command echelons as the battle changes. This concept gives the commander in the best position to make effective decisions the control needed to be effective.[11] The processes involved in migration of control have not been effectively defined, but the concept shows some promise. An example of a similar situation is the migration of the control of fires during an air assault. The Escort Flight Leader (EFL) begins with control of fires, at some point they are passed to the Forward Air Controller (FAC), who has the discretion to push and pull control to a Forward Air Controller (Airborne) (FAC(A)) asset. This evolution generally runs smoothly because it is understood and trained to by all parties involved, and migration of control of the larger battle could follow a similar pattern.

c. Control of Information

Because NCW is dependant on robust and constant communications, there is a concern that control of forces will be tightly held by the most senior commander instead of being distributed to the forward small unit commanders. Senior members of both the Navy and Marine Corps have expressed concerns about this effect and hope to prevent senior officers from micromanaging the battle. The Marines have suggested preventing certain flows of information entirely to insure that leaders are not reaching to far down the chain of command when they should not. The

[11] Dr. Alexis Levis, Private Communication, 16 March, 2004.

concern is that a general officer or admiral may become concerned with specific tactical engagements instead of fighting operational battles. The Marines are extremely concerned about keeping the "General's out of the fighting holes."[12] Micromanagement facilitated by robust communications is not the desired result of NCW; in fact NCW espouses the opposite. It will be important to not only exchange the right information while conducting NCW, but also to not exchange unnecessary and detrimental information so that junior leaders are free to take appropriate action in response to changing situations on the battlefield.

3. Command and Control

a. Definitions

Command and Control are difficult terms to define and separate. JCS Pub 1 defines command as the

> responsibility for effectively using available resources, planning the employment of, organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions. It also includes the responsibility for health, welfare, morale, and discipline of assigned personnel.[13]

Alberts and Hayes note that "this definition subsumes control as a part of command."[14] They go on to discuss problems with drawing distinction between command and control, concluding that "much of the discussion is focused on a single commander, the one in charge. In fact, command and control in modern warfare is a distributed

[12] Futures Department, Marine Corps Combat Development Command (MCCDC), Private Communication, 17 March, 2004.

[13] JP 1-02, Department of Defense Dictionary of Military and Associated Terms.

[14] David S. Alberts and Richard E. Hayes, *Power to the Edge*. (Washington: Department of Defense, 2003), 14.

responsibility."[15] They assert that forces fighting Network Centric Warfare no longer have a single commander controlling a large force, but have the responsibility for conducting command functions spread out over connected operating forces. This view of command conflicts with the current system where commanders have a legal responsibility that cannot be delegated.

Alberts, Gartska, and Stein say that "the very essence of command and control lies in the ability of the commander, at any level, to make the most of the situation."[16] They further explain that the output of command and control is the flow of the battle and the successful completion of military objectives. Whether command is centralized or distributed becomes less important than the output of the command and control process. Again, this version eliminates the requirement for a single commander responsible for leading forces as long as a desirable outcome can be achieved. They assert that a Network Centric command and control process will give a superior output for the following reasons:

1) decision entities or C2 elements will be more knowledgeable;

2) actor entities will be more knowledgeable;

3) actor and decision entities will be better connected;

4) sensor entities will be more responsive; and

[15] Ibid.

[16] David S. Alberts, John J. Gartska, and Frederick P. Stein, *Network Centric Warfare*. (Washington: Department of Defense, 1999), 157.

5) the footprint of all entities will be much smaller.[17]

The above arguments make two critical assumptions: access to more information will make an entity more knowledgeable, and more knowledgeable entities will take better action than less knowledgeable entities. These are reasonable assumptions, but are by no means infallible. It is easy to make an argument that increased data does not equate to more knowledge. A man with two watches is never sure what time it is, but a man with one watch is. Also, more knowledgeable entities may not act better, especially if decision entities and actor entities see conflicting courses of action.

b. Self-Synchronization

Network Centric Warfare attempts to operationalize the idea of distributed command functions through the concept of self-synchronization, which is defined by Cebrowski and Gartska as "the ability of a well-informed force to organize and synchronize complex warfare activities from the bottom up."[18] The potential value of this concept is hard to argue with as defined above, but the definition is vague and offers no understanding as to what exactly self-synchronization is or how it can be achieved. Alberts, Gartska, and Stein help narrow the definition by explaining that "Self-Synchronization is a mode of interaction between two or more entities,"[19] and requires

---

[17] Ibid., 158.

[18] Arthur K. Cebrowski and John J. Gartska, "Network Centric Warfare: Its Origin and Future," *Proceedings of the U.S. Naval Institute,* January 1998

[19] David S. Alberts, John J. Gartska, and Frederick P. Stein, *Network Centric Warfare*. (Washington: Department of Defense, 1999), 175-176.

> two or more robustly networked entities, shared awareness, a rule set, and a value adding interaction. This combination… enables entities to operate in the absence of traditional hierarchical mechanisms for command and control.[20]

Alberts and Hayes state that the assumptions for self-synchronization are:

- Clear and consistent understanding of command intent;
- High quality information and shared situational awareness;
- Competence at all levels of the force; and
- Trust in the information, subordinates, superiors, peers, and equipment.[21]

They assert that with the appropriate information and training, disparate units can self-synchronize and conduct complex warfare activities from the bottom up.

4. Problems

a. Command and Control

Distinctions between command and control are hard to define and are often self-referential. Some would claim that command is what commanders do and control is what non-commanders do. Others may say that commanders are people who command. This problem with distinctions helps lead to what Alberts and Hayes call "inappropriate defenses of tradition, hero worship, and a misunderstanding of the enduring nature of command and control"[22] Pigeau and McCann offer the following distinction:

---

[20] Ibid.

[21] David S. Alberts and Richard E. Hayes, *Power to the Edge*. (Washington: Department of Defense, 2003), 27.

[22] Ibid., 14.

- Control: those structures and processes devised by command to enable it and manage risk.

- Command: the creative expression of human will necessary to accomplish the mission.[23]

What is lacking from the above discussion of command and control is a sense of responsibility. Command functions, such as planning, organizing, and controlling forces, may be distributed, but command as a responsibility should not be. Command is more than an idea of how to employ troops on the battlefield, it extends off of the battlefield to peace times and includes a responsibility for all that those under one's command do and fail to do. Command also entails a legal responsibility for personnel, equipment, and decisions. Control of troops includes employment during battle and the processes to enable command decisions, but it does not include the responsibility associated with command. Although the above is a hardly a formal definition, it highlights that part of the equation has been removed from many discussions of Network Centric Warfare.

b. Self-Synchronization

If one accepts that given the required elements for self-synchronization units can self-synchronize, what does it really mean? How do self-synchronizing units determine what actions need to be taken and what forces will conduct them? The delineation of objectives and allocation of forces is traditionally a command function. Who conducts this function in a self-synchronizing force? Alberts and Hayes explain that

[23] Ross Pigeau and Carol McCann, "Re-conceptualizing Command and Control," *Canadian Military Journal Vol 3, No. 1*, Spring 2002, 57.

> The command function is not absent in self-synchronized forces; however, it does depend on achieving congruent command intent, shared situational awareness, authoritative resource allocation, and appropriate rules of engagement, as well as similar measures that guide but do not dictate details to subordinates.[24]

This statement implies that the command function (what commanders do) in addition to decision making authority is distributed amongst the self-synchronizing units, and that separate units can come together to resolve real-time disputes. It also assumes that initial guidance is given by a higher echelon and carried through by the self-synchronizing forces with no additional interaction between echelons. With a distributed command function as defined above, it is neither clear where the congruent command intent comes from, nor who is responsible for determining if objectives have been met or need to be changed.

The above vision of self-synchronization does not clearly explain how forces will self-synchronize. One problem is that the traditional command functions are divorced from actual commanders with the assumption that all units will be led by competent leaders and will not require a higher commander for action. This assumption is partially grounded in the belief that equally trained units, when faced with the same information about command intent, friendly disposition, and enemy disposition, will collaborate to agree on a common course of action. There continues to be much debate about the ability to share information in real time so that separate units will have

[24] David S. Alberts and Richard E. Hayes, *Power to the Edge*. (Washington: Department of Defense, 2003), 27.

the same information, and this will be addressed later. Assuming that the technical problem of sharing information is solvable, even with the same information, leaders will not always come to common conclusions about their situation (shared situational awareness) nor be able to reach agreement on a common course of action. In fact, disagreement about the correct action is the norm in military operations not the exception. Self-synchronization assumes away the responsibility for arbitrating disagreements between self-synchronizing units by distributing the command function among many coequal entities.

Alberts, Hayes and others have noted that with no single commander responsible for performing command functions (allocation and reallocation of resources, choosing courses of action, determining priority of objectives, etc.) distributed forces may lose their ability to act as a coherent force and tip into chaos. The arguments against forces tipping into chaos generally involve training and shared information with the belief that well trained units with the same information will always agree to take the best action.[25] This argument is insufficient in that the real defense against tipping into chaos is command oversight by tactical commanders who purposefully maintain integrity of forces. Even with identical training and information, two units engaged in direct tactical action may not respond to real time changes on the battlefield in like manner and often will have conflicting short term priorities. Even if engaged units are able to respond to changes in the situation, their

[25] Ibid., 97-127.

actions will be largely controlled by their level of engagement and their local perspective. It can be argued that it is human nature to deal with the most pressing problems first, especially when one's life is at risk. Even if information about a new or different threat is made available, a leader engaged in combat may not give away supporting assets, redistribute forces, or sacrifice his troops to meet this new threat. A higher level tactical commander must be responsible for making those decisions to ensure that the force can continue to fight.

B. FORCENET

1. Definitions

The US Navy has stated that it will operationalize Network Centric Warfare through FORCEnet. The official definition of FORCEnet, as adopted by the Commander, Naval Network Warfare Command, is:

> FORCEnet is the operational construct and architectural framework for naval warfare in the information age that integrates warriors, sensors, networks, command and control, platforms, and weapons into a networked, distributed combat force that is scalable across all levels of conflict from seabed to space and sea to land.[26]

This definition is all-encompassing and is intended to imply that FORCEnet is not just a communications network; it is the entire, fully networked naval force. However, the above definition has not been fully accepted within the Navy, Marine Corps, Systems Commands, or DoD contractors. The Naval Transformation Roadmap states

> FORCEnet is the operational construct and architectural framework that will provide the

[26] Chief of Naval Operations Strategic Studies Group XXI, *Accelerating FORCEnet – Winning in the Information Age.* (2002), 1-2.

> capability to deliver persistent and comprehensive surveillance, rapid networked command, and common, accurate battlespace picture necessary to support decision making at a tempo that overwhelms an adversary's capability to react and respond.[27]

This definition narrows the scope of FORCEnet to an information architecture and not a total force concept, but it is still an ambitious, overarching view of what FORCEnet should be. The implied assumption in the Naval Transformation Roadmap definition is that by building the technological architecture for moving and delivering information, creating a common battlespace picture, and supporting decision making at appropriate levels, a netted force capable of conduction Network Centric Warfare will emerge.

The important distinction between the above definitions is that the Naval Transformation Roadmap removes the organization and employment of forces from the FORCEnet picture. FORCEnet can exist separately from the forces that use it and from their method of employment. This view is consistent with the Sea Power 21 concept quoted in Chapter I.

2. Vision versus Reality

a. Sea Power 21

FORCEnet is viewed as the glue that unites Sea Strike, Sea Shield, and Sea Basing in the Sea Power 21 vision[28]. The Navy Warfare Development Command (NWDC) has broken the four pillars of Sea Power 21 into Mission

[27] *Naval Transformation Roadmap 2003: Assured Access & Power Projection…From the Sea (Sec D.).* (Washington: Department of the Navy, 2003), 63.

[28] Adm. Vern Clark, "Sea Power 21," *Proceedings of the U.S. Naval Institute,* October, 2002

Capabilities Packages (MCP) and further into Envisioned Capabilities (EC).[29] Figure 1 shows how the pillars are broken into MCPs. The three MCPs for FORCEnet are ISR (Intelligence, Surveillance, Reconnaissance), COP/CTP (Common Operational Picture/Common Tactical Picture), and Communications and Data Networks.

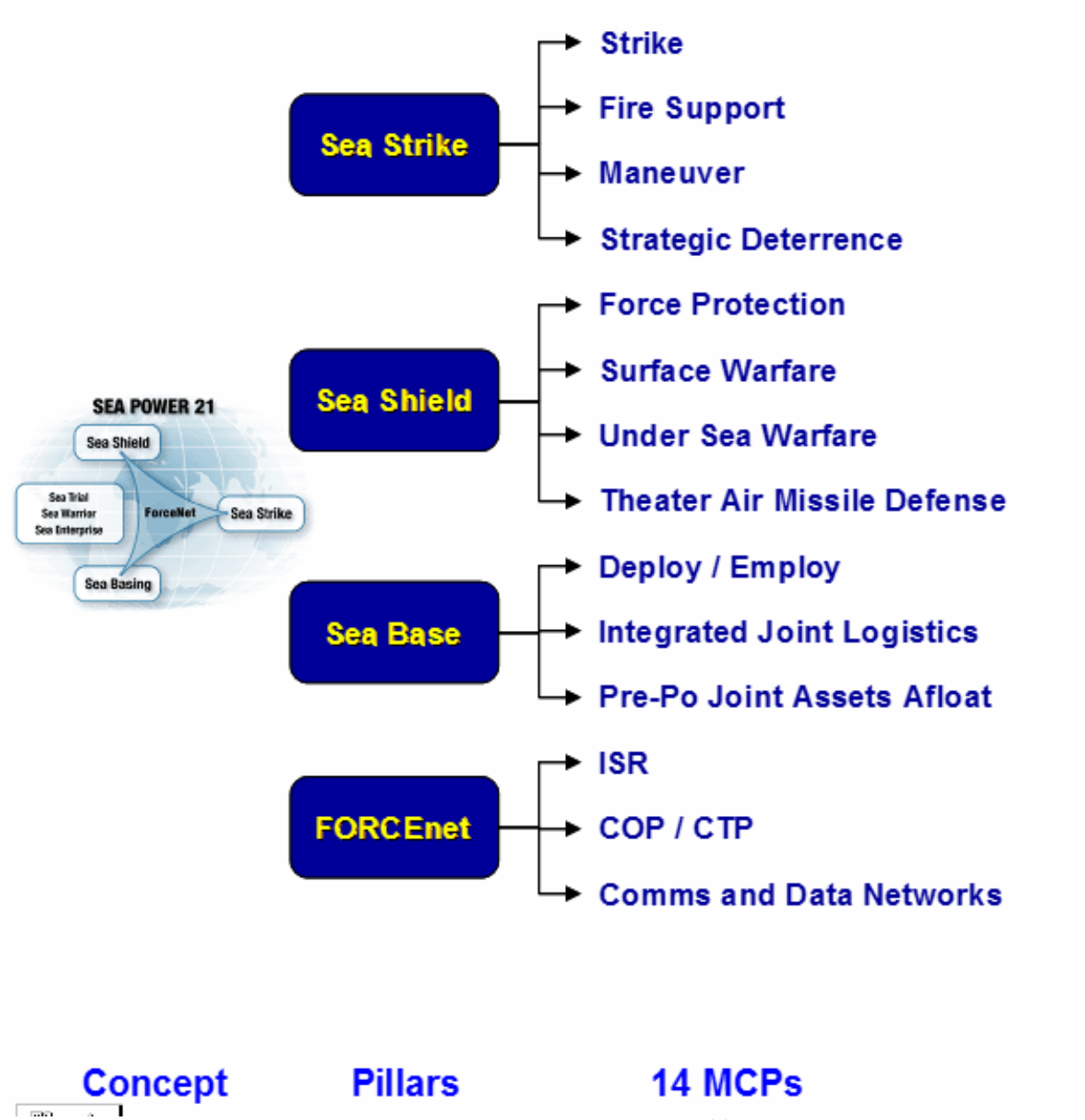

Figure 1. Sea Power 21 MCPs[30]

[29] FORCEnet Brief, Navy Warfare Development Command, January 2004.

[30] Ibid.

These three FORCEnet MCPs are broken into 14 Envisioned Capabilities as shown in Figure 2. The FORCEnet MCPs exclusively concern data collection (ISR), data integration (COP/ CTP) and connectivity (Communications and Data Networks), which are all essential to FORCEnet. The missing elements as envisioned by the Strategic Studies Group XXI definition are decision aids, cognitive aids, force organizations, and command and control structures. Simply connecting units and sharing data will not yield the "orders of magnitude improvement" that FORCEnet and NCW promise. New ways of organizing and employing units are also necessary. Decision and cognitive aids are vital to sifting through the potential soup of information that can be generated in a highly connected system. The MCP and EC breakdown of Figure 2 serves to further define down

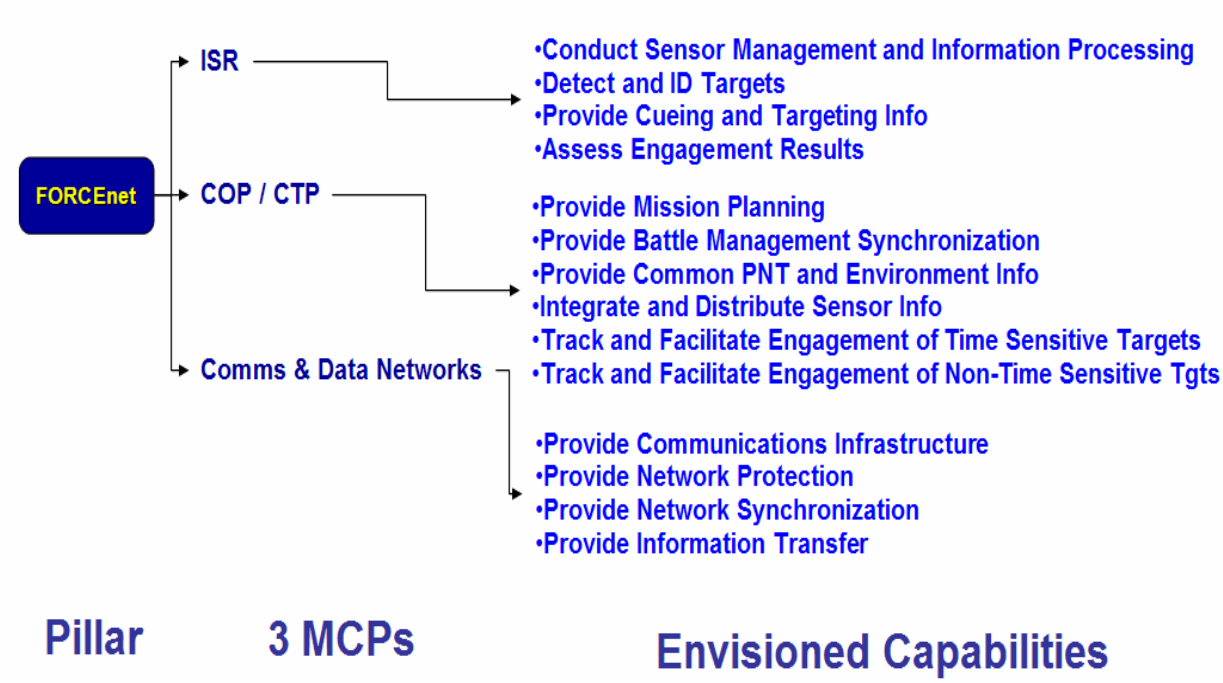

Figure 2. FORCEnet MCPs and ECs[31]

[31] Ibid.

FORCEnet to a war time internet. This vision is attractive because it is primarily an engineering problem that can be funded and purchased. The problem is that without a larger vision of employment, the systems built may not bring any additional capability to the battlefield.

b. Command Organizations

Depending on which definition is used, self-synchronization attempts to distribute either the command function or decision making authority among lateral units. This technique can be beneficial in short term tactical environments, but has the potential to present major problems at higher levels. One important consideration is that FORCEnet must preserve the legal concept of command. Commanders are legally responsible for all that their subordinates do and fail to do. Commanders cannot delegate their responsibility, but traditionally have delegated authority to subordinate leaders. Some advocates of self-synchronization see a military that does not have commanders responsible for their subordinates in the same manner. When Alberts and Hayes discuss distributing the command function, they are also distributing the responsibility of commanders.[32] This is a radical departure from traditional military command organizations and may be unachievable for a large force. The Navy and Marine Corps must be careful not to radically limit the responsibility of commanders when attempting to build a Network Centric Warfare capable force.

3. Common Pictures

One key attribute that FORCEnet must possess is the ability to provide a common battlespace picture. For a

[32] David S. Alberts and Richard E. Hayes, *Power to the Edge*. (Washington: Department of Defense, 2003), 27-31.

common picture to be valuable it must be able to display desired information accurately, in real-time, and clearly enough that commanders can quickly use the information. There are several recognized problems with developing common pictures. The latency problem involves the ability to keep common pictures updated in real-time. Because any information must be sent from the reporting source, to the common picture, and then to the user, there is a delay in transfer of information. When satellites are used to relay information, this delay can be substantial. It is possible for two users to have different pictures based solely on their distance from the common picture transmitter. Another problem is that the same information is often reported by multiple sources. This double reporting can result in a single piece of data (for example, an enemy unit) being duplicated multiple times over. A similar problem is that two reporting sources may report slightly different information with no system for immediately determining which is correct. For example, source A reports a reinforced platoon-sized force at grid 123456 and source B reports a company minus sized force at grid 123460. Each report may refer to a separate group of enemy troops, or they may both be reporting on the same force at different locations. The ground truth cannot be immediately determined until some form of verification is done.

Another, more fundamental, problem with common pictures is that there is little agreement on what they should contain. Some common pictures are a storehouse for all information; others give targeted pictures of only certain pieces of information. Several varieties of common

pictures have been proposed. The two most common types are detailed below, and Figure 3 highlights some important differences.

a. Common Operational Picture

The Common Operational Picture, or COP, is the most commonly discussed common picture and is often used to mean a generic common picture. Not all versions of the COP are the same, but the Defense Information System Agency views the COP as a single repository of all available information for the operational level commander. The COP is configured in its development and is largely not changeable by the user. This model has fallen out of favor recently because of its "one size fits all" design, command push architecture, and inefficient use of bandwidth.[33] The cornerstone of the COP is that it is truly common for all users, but it lacks flexibility in use and display that users need.

b. User Defined Operational Picture

The User Defined Operational Picture, or UDOP, is a more flexible version of the COP. Many data integration and data display engineers have abandoned the COP for the UDOP. UDOPs are configurable and reconfigurable by the users to present only the information that a user asks for. They are built on a "on demand" architecture that looks for the information that a user requests. They can contain any information available to the system, but the user only receives the information that he requests. One failing of the UDOP model is that it presents the user only what the

[33] Rob Walker, "GIG Enterprise Services Piloting," Defense Information Services Agency, April 20, 2004

user asks for, and there is no way for the user to get information that he does not know he needs.[34]

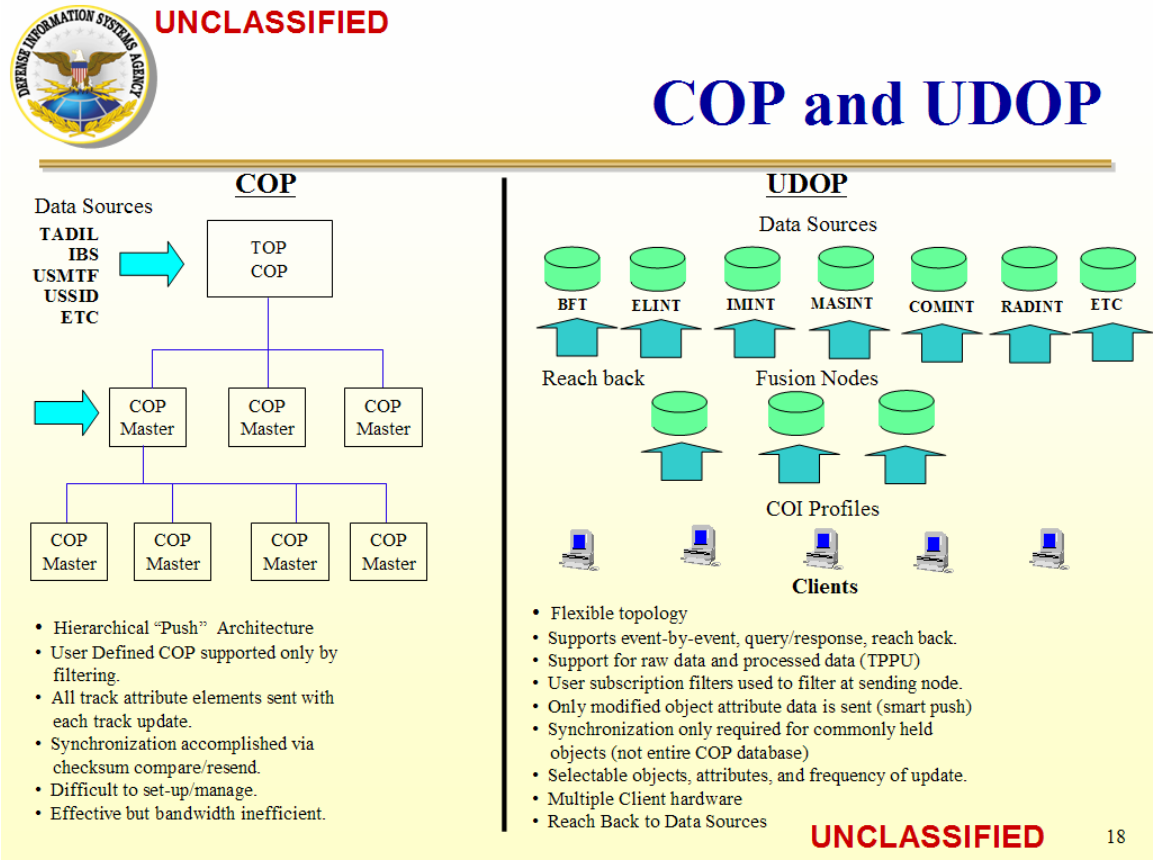

Figure 3. COP and UDOP[35]

C. STATE OF TECHNOLOGY AND EMERGING TECHNOLOGIES

1. Technological Areas

The emerging technologies presented here have been broken down into five areas. These areas represent what a person does with information. First, the information must be gathered. This can be done through the five senses, through external sensors, from Intelligence Analysts, or from a computer system. Once the information is gathered, it must be processed. This can be done internally, by an analyst, or by an automated system. After the information is processed, or sometimes before, depending on time

[34] Ibid.

[35] Ibid.

constraints, the user must decide or act upon the information. This decision may be to take a specific action, take no action, gather more information, do more processing, or ignore the information entirely. At some point the user will need to move the information. This may simply be from the gathering asset (sensor) to the processing asset (analyst), or it may be moving it to another command or unit. While he does all of this, the user must protect the information. Protection is more than just standard Information Assurance and Security, but also includes ensuring the timeliness of the information and its pedigree. Technological concerns will be broken into the above areas of gather, process, move, decide, and protect.

2. Gather

This thesis does not focus on gathering or sensing assets or technologies. The state of the art in this area is rapidly evolving and is beyond the scope of this work. It is assumed that sensors exist that can place useful information into the FORCEnet architecture. This thesis addresses the information once it has left the sensor.

3. Process

a. Computing Power

Computer processing power has obeyed Moore's Law since the invention of the silicon microprocessor. Moore's Law states that the number of transistors that a microprocessor manufacturer can place on a chip doubles about every two years. As a result, computer processing speed will go up while cost will go down.[36] Moore recognized that this trend would slow down and eventually level off as transistors became so small that quantum

[36] Dorothy E. Denning, *Information Warfare and Security.* (New York: ACM Press, 1999), 294-295.

effects and the size of atoms would interfere with the operation of transistors. However, modern parallel computing schemes are encountering a different problem. Because these computers can use dozens, and soon hundreds, of single processors and have reached the teraflop range in clock speed, they can perform calculations faster than they can access memory. Memory access is limited by the speed of light and the physical distance between the memory storage location and the chip conducting calculations. Work is being done by some IT companies to shorten physical distances in computer processors, but the speed of light problem will eventually limit the growth of conventional computing power[37].

b. Smart Materials

Non-silicon computing has seen some recent interest thanks to new photo-reactive and electro-reactive materials. These "smart" materials are used in place of traditional computing components to create wearable computers and power sources. Electric "muscles" are made of materials that expand when a current is applied, and when physically contracted will produce a current. In laboratory experiments, these materials have been shown to be reliable enough to be used as a low current power source. Also, these "smart" materials can be woven into fabric to create basic analog and digital computers that can do basic calculations, store data, and even play music. Although far from a mature technology, "smart" uniforms may be used in the future for forward units[38].

---

[37] Presentation, HP Labs, March, 2004.

[38] Dr. Neil Gershenfeld, Director Center for Bits and Atoms at MIT. Private Interview.

c. Metadata

Metadata is information about data and is an important element in building the FORCEnet network. Much the work in fusing and integrating FORCEnet data assumes that pieces of data can be tagged so that the system knows how to process them. There are several languages in use now with this capability, such as the Extensible Markup Language (XML). Each language has its own capabilities and limitations, but one consistent problem is that by tagging data the amount of bits needed to represent the data grows proportionately. As a result, the use of metadata greatly increases the bandwidth requirement for any given piece of data. For example, a forward unit wishes to send an enemy grid coordinate back to a higher command echelon. The eight digit alpha numeric grid coordinate (i.e. AB123456) nominally takes up a defined number of bits depending on the encoding scheme used. However, the data needs to be tagged with additional information to be useful to the system. Some metadata tags include time sent or sending unit. As the data move up through the network as explained in the Chapter IV, additional tags may be added at each level. These additional tags will each increase the size of the data packet.

The problem of increased data size is greatly overshadowed by the utility of metadata tags. Competing or conflicting pieces of information can have tags which identify:

- Time created,
- Time transmitted,
- Source,

- Whether or not it has been verified,
- How it was verified and by whom,
- Which units have used the data.

Other pieces of important metadata can be built into the tagging architecture as necessary. This capability allows information to have a verifiable pedigree so that decision makers know which pieces of information may be most relevant or reliable in a given situation.[39]

4. Move

a. Communications on the Move

A large amount of work has been done in the DoD to improve bandwidth for digital communications to tactical units. Ships and aircraft have several promising programs to greatly increase over the horizon communications bandwidth (fiber-based terrestrial bandwidth is not a limiting factor) but little progress has been made to solve the "comms on the move" problem for infantry and land vehicles. Programs like the Joint Tactical Radio System (JTRS) have made large promises that have so far been unrealized, and mobile satellite receivers suffer from the "pointing problem," keeping a moving vehicle in the satellite footprint and pointing in the right direction.

These problems come from the fact that over-the-horizon communications in the field can presently only be accomplished through satellites. In order to achieve a high bandwidth signal, higher frequency signals are needed. These are line of sight and cannot be used for over-the-horizon communications without some means to relay them. Traditional over-the-horizon communications, such as HF

[39] United States Geological Survey, "Metadata in Plain Language." Located at http://geology.usgs.gov/tools/metadata

have insufficient bandwidth for digital communications. Some work has been done in building Unmanned Aerial Vehicle (UAV) relays in the form of BAMs and HAUAVs. Other proposed solutions include "TacSats" (very low orbit satellites that can be launched by field commanders as needed)[40], and field-expedient cell towers. These concepts are currently very immature, but show promise for the near future. Any of these relay platform at lower than orbital altitudes offer some significant advantages and disadvantages compared to satellite communications. Constellations or groups of UAVs or TacSats can be quickly put up in desired locations, moved as the battle moves, and reconstituted if electronically attacked. They require less transmit power both at the surface and on board and they are local assets that do not have to compete with national requirements although deconfliction of airspace and frequency bands would still be required.[41]

b. Bandwidth Aggregation

Another approach to the bandwidth problem involves better management of the bandwidth that is already available. Prototypes have been built that can manage three or more sources of bandwidth to transmit information though the best available source. If a high bandwidth connection is lost, the program automatically adjusts to use the next best available option. These systems do not simply use one source at a time, but can aggregate bandwidth and utilize it all as one big "pipe." These concepts, when coupled with Content Shaping (below) allow a commander to use available bandwidth for routine purpose

[40] Frank Morning, Jr., "Smallsats Grow Up," *Aviation Week & Space Technology*, December 8, 2003

[41] Ibid.

(such as emails home or internet browsing) while ensuring that critical communications (such as orders and intelligence reports) are transmitted [42]

c. Always Best Connected

Always best connected algorithms are becoming common in the wireless community. They allow a system to check for various ways to connect to a desired node and choose the best one available. As conditions change, the system continually updates to the best connection available. As these algorithms get better, they will allow systems forming ad hoc networks to constantly stay connected and quickly switch between pathways without user input.[43]

d. Routing Scheduling

In addition to always best connected algorithms, routing scheduling can help maintain connections at the highest bandwidths available. Routing scheduling will dynamically switch between Code Division Multiple Access (CDMA) and Time Division Multiple Access (TDMA) depending on which coding technique provides the best service to the user. As electronic traffic changes, along with environmental conditions and data types, the coding scheme for any given signal can adjust so that the best connection with highest possible throughput is maintained.[44]

e. Content Shaping

Content Shaping is an effort involving the ability to automatically adjust the information that is sent between users to the size of the bandwidth available.

---

[42] UC San Diego California Institute for Telecommunications and Information Technology, Demonstration, 19 February, 2004.

[43] Ibid.

[44] Ibid.

Transmitting locations, such as websites or data nodes, can determine the bandwidth available and adjust the data sent accordingly. This is more than changing transmitting speeds, but includes changing the content that is sent. An example is compressing streaming video to lower quality when a high speed connection is lost. A low bandwidth submarine can hit the same site as a high bandwidth fiber user and get the same critical information, but in a different format. This concept can also be coupled to an "always best connected" algorithm to not only ensure connectivity but also that important information is transferred. By shaping the content transmitted, a user can also prioritize traffic so that during high traffic, low bandwidth environments, only high priority traffic is sent and the rest ends up being dropped or buffered.[45]

5. Decide/Act

The field of decision aids is a very crowded and varied discipline. Most "decision aids" are actually better information aggregation systems. They do not "aid" the decision maker in the sense that they analyze outcomes or present alternatives, but instead present information to the decision maker in a better format. These types of decision aids could be more accurately described as situational awareness aids in that they help users get a clearer situational picture faster and are quickly becoming more and more user friendly. Some companies have used directional sound, 3-D immersion, and bio-mechanical techniques to improve the information transfer process. Other types of decision aids are designed to actually help the decision maker come to a better decision. A few are discussed below.

[45] Ibid.

a. Simulations and Information Pedigrees

Several companies have started to attempt to use computer simulation to help decision makers reach a desired outcome. These simulations are currently not usable on a tactical scale, but have begun to show promise especially in network modeling. At strategic and operational levels, these models can help planners test a variety of plans and see projected outcomes. These simulations will become very important as the pace of battle increases. Early simulations are being used in air and missile defense commands and may soon be making tactical decisions about which targets are friendly and hostile.

As computer-aided decision aids get more advanced, it becomes important to be able to identify the pedigree of pieces of information and recommended courses of action. Algorithms can identify which pieces of information were used to reach a given conclusion, and identify how the conclusion would change if certain elements of information change or are proven false. By identifying critical elements of information, decision makers can recognize how a recommendation was reached and determine if a suggested course of action is still valid. This concept can help prevent cascading assumptions that lead to decisions based on guesswork and no real data

b. Always Best Located

The DoD and the world at large widely recognize that U.S. reliance on Global Positioning Satellite (GPS) information is a potential vulnerability. As GPS signals become easier and easier to deny in specific geographic locations, new techniques for targeting and navigation are needed. One attempt is the Always Best Located algorithm.

In addition to being able to tie in multiple navigation systems (GPS, INS, etc) this algorithm can do GPS over IP to a surprising degree of accuracy. By using a GPS receiver in the San Francisco Bay area, researchers at University of California San Diego can transmit data over an IP network and get 50 meter accuracy. This degree of accuracy is insufficient for some targeting algorithms, but is definitely good for navigation. In the near future an asset out of the theater may be able to receive GPS data and transmit data to an asset in a GPS denied area that is sufficient for targeting.[46]

6. Protect

The field of information and network security is far too vast to be addressed in this thesis. Many different techniques are available for security that range from object level security to low probability of intercept communications. The triad of computer security consists of availability (sometimes called access), confidentiality (sometimes called secrecy), and non-reputability. Each of these elements has its own problems and solutions with some interesting work being done. In addition to computer security, there is also a security concern with military information. True multi-level security systems have been designed, but none have been successfully deployed for a variety of reasons. Below are a few important points concerning a huge field of work.

a. Dissimilar Redundancy and Reconstitution

A growing concern within the DoD is the US military's inability to fight in a "lost comm" condition. As smart systems become more and more reliant on networks and communication, their vulnerability to attack grows as

[46] Ibid.

well. This problem grows exponentially as the services acquire more and more joint systems that use the same techniques for passing information. For example, if all systems rely on C band satellite communications, what happens when the C band is denied? Likewise, as digital communications moves toward IP, how does information get passed when the IP network is shut done? To improve the probability that a highly networked system will stay connected, a series of dissimilarly redundant communications capabilities can be imbedded. Dissimilar redundant communications allow at least a minimal level of connectivity in a non-permissive environment and should be considered during the design of new systems. In addition to dissimilar redundancy, reconfigurability can help to maintain a networked system. Both communication hardware and software need to be able to be restored after an attack. If satellites are destroyed, there needs to be a way to restore over-the-horizon communications to ensure access to the networks is not lost.

b. Encryption

Modern encryption algorithms remain ahead of modern cracking algorithms. However, this advantage will not last for long[47] as cheap computing power continues to become available. Asymmetric encrypting schemes are of immediate concern because of the lack of mathematical rigor related to them. Mathematicians have been unable to quantify how difficult a problem the RSA encrypting scheme, and all similar schemes, is to solve. The problem is that RSA is based on large number factoring which has never been proven to be a difficult or unsolvable problem. If a

[47] Dorothy E. Denning, *Information Warfare Security.* (New York: ACM Press, 1999), 294-295.

bright young mathematician were to develop a very fast algorithm for large number factoring, RSA would be rendered useless overnight. A potential successor is the Elliptical Curve encryption algorithm. It is transparent to the user which algorithm is involved, but the Elliptical Curve has the advantage of mathematical rigor behind it. This scheme can be proven to have an appropriate level of difficulty and can be easily adjusted as computing power increases.[48]

c. Multi-Level Security

In many circles of the DoD, multi-level security is discussed in the same tone as unicorns and elves. A true multi-level security system may never be developed, but there are some ways around the problem during a military campaign. A proposed solution is derived from the classification process of operational information. Operational information is classified for one or both of the following reasons: the information itself is classified, or the source that collected it is classified. Often, the important pieces of information, enemy location and disposition, enemy activity, etc., is unclassified but cannot be passed to the field commanders because of the source or other ancillary information. A potential workaround is to have a classified clearing house that identifies which pieces of information are classified and tag them to their appropriate level. Data can then be sent through channels with classified portions stripped off the message where appropriate. This technique would allow a corporal to receive the information that an enemy tank column is heading for his position without knowing that it came from a CIA operative. This idea can be extended so

[48] Chris Oakes, "Getting Ahead of the Elliptic Curve." Wired News, Wired.com. January 13, 1998.

that information sharing with coalition partners and non-government agencies can be controlled in a similar manner. The difficult part of implementing this concept is identifying the rules for tagging pieces of information. If the “business rules” can be developed, the technological application would be relatively simple.

Another potential workaround is that operational intelligence often has a lifetime attached to it. The position of friendly assets from three weeks ago may no longer be useful to anyone after they have moved. Classification standards do not account for the time-sensitive nature of this type of intelligence, and information sharing could be greatly improved if lifetimes were attached to classification levels. An example would be that the location and disposition of an enemy logistics point is reported by a Special Operations unit in the vicinity. The unit then departs, but their report remains classified. Once the unit is gone, there may no longer be useful information for the enemy in the report, but friendly commanders may not be able to access the information because of a past classification of the information. A lifetime attached to the classification would help this problem. Again, the difficulty lies in establishing the “business rules” for implementing this type of system and determining when a report no longer requires classification.

D. PROBLEMS

1. Shortfalls in Vision

Both Network Centric Warfare and its instantiation in FORCEnet are ambitious visions. They also both have some significant shortfalls. Some advocates of NCW attempt to

divorce NCW from tactical command and control by employing self-synchronization as a replacement for traditional command functions and attempt to eliminate, or at least marginalize, the importance of unity of command. These two concepts have the potential to promote chaos on the battlefield and remove the ability of a military unit to produce coherent effects.

The FORCEnet vision suffers from a lack of agreement on its definition throughout the Department of the Navy. This disparity has led to the "Big FORCEnet, Little FORCEnet" paradigm in OPNAV and elsewhere. Big FORCEnet has come to mean the full spectrum vision put forward by the SSG, while Little FORCEnet is the physical network that connects units. Little FORCEnet is addressed by the MCPs in Figures 1 and 2 above and can be procured as information systems. Big FORCEnet is much harder for the Navy to get its hands around and is nearly impossible to develop through the normal procurement process. Without a unifying vision for Big FORCEnet, Little FORCEnet is being built in an ad hoc and piecemeal fashion.

THIS PAGE INTENTIONALLY LEFT BLANK

III. PROPOSED TOPOLOGY

A. OVERVIEW

1. FORCEnet

As referenced above, FORCEnet has multiple definitions that range from just a military internet to the all encompassing vision of SSG XXI. Here, the FORCEnet information topology refers to the design of the computer network and its associated communications requirements; however, this does not imply that FORCEnet is only the computer and communications networks. At some level, FORCEnet needs to have a communication network in place to move information between users, but FORCEnet itself can and should be much larger. The design of the network needs to match the intended use of these communications and computing assets. The communications network, or Little FORCEnet, cannot be built without regard to its use.

By addressing the larger or higher level issues of the FORCEnet network's employment, a better information movement system can be designed. Technical concerns obviously need to be addressed, but FORCEnet is not just a technical undertaking. The organizational structure of units employing FORCEnet, as well as the type of operations in which FORCEnet will be employed, needs to be addressed in order to ensure that the final product can meet the requirements of the operating forces.

2. Common Pictures

Common pictures are often confused with common views. This may be a semantic argument, but it is presented here for clarity when discussing common pictures below. The impetus behind the design for the CROP and UDOP was that

the one-size-fits-all COP was unwieldy for commanders[49]. Too much information or extraneous information cluttered the COP, and commanders at multiple echelons were not able to effectively sift through the information. A popular solution to the information overload problem has been to combine a "publish and subscribe (pub-sub)" system with the COP. Units that produce information will publish products to a common database and consumers will subscribe to the information that they need. The pub-sub construct is employed in most CROP and UDOP models. This solution works well to limit the amount of information presented to a user to a manageable amount.

The problem with the pub-sub construct as employed by most UDOP and CROP models is that there is no single, complete, integrated picture. Each user chooses which pieces of information to view, but nowhere is complete integration done. FORCEnet needs to have a single complete picture within the system to maximize the benefit of drawing information from multiple sources. Users may select how they view the common picture by selecting which aspects they need to see, but the picture exists in and of itself. Here, when speaking of a common picture, it is implied that the picture is a complete, integrated picture of the operating environment. Under this construct, a UDOP would be a User Defined Operational View (UDOV) that selects which pieces of the common picture need to be displayed (see Figure 4).

[49] Rob Walker, "Evolution to Net-Centric Operations," Defense Information Systems Agency.

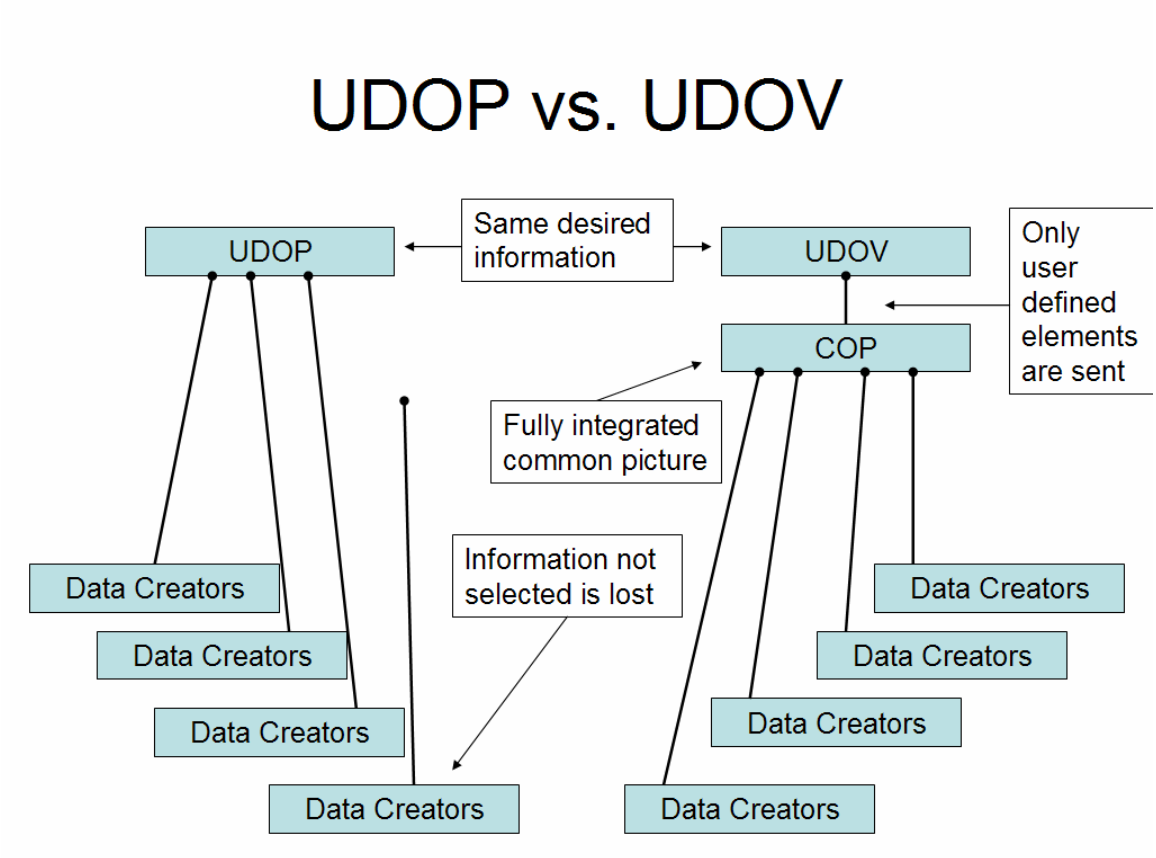

Figure 4. UDOP vs. UDOV

B. FOUR-TIER MODEL

The FORCEnet network, as proposed here, is a network of networks. Each command from the lowest practical level has its own network for sharing information. These networks are connected with each other along organizational and functional lines. Additionally, ad hoc connections are available to be established and broken as needed to conduct missions. This model is designed to be an operational and tactical network, but it can easily be extended in scope to cover administrative concerns as well.

The basic topology of the proposed FORCEnet network is a four-tier structure. Each tier of networks performs similar functions at different levels of granularity. This design allows commanders to maintain control of their units

while not interfering with self-synchronization of forward units. Information exchanges between levels are governed by business rules agreed upon by appropriate commanders. Information is exchanged through either standard or on-request exchanges which are explained in greater detail in Chapter IV. The four-tier model is designed to separate types of information to aid users in finding important pieces of information. A tactical unit needs information relevant to the current tactical picture and is not immediately concerned with civil unrest elsewhere in the world. A strategic commander may be interested in that civil unrest because it will affect the apportionment of his assets. These distinctions between types of valuable information are captured in the four-tier model so that the right information is delivered to the right people at the right time.

1. Common Strategic Network (CSN)

The Common Strategic Network is owned by the Commander in Chief and is operated at the Department of Defense level. This CSN ties together strategic information from all national level assets and supports the Regional Combatant Commanders. The CSN is intended to support all elements of national power by interfacing with all relevant government agencies (CIA, FBI, State Department, etc.). Business rules for sharing information across agencies are arbitrated and agreed upon by the appropriate representatives, and these rules are designed into the system. The CSN is a military network, so appropriate legal issues regarding sharing information have to be accounted for when the business rules are established. The

purpose of the CSN is to provide strategic level commanders the support they need to give strategic level guidance to lower echelon commanders.

The CSN is directly linked to all active Common Operational Networks (CON, see below), and information is shared as necessary (exact information sharing requirements will be discussed in Chapter IV). A key feature of the CSN is the Common Strategic Picture (CSP). The CSP contains a real time, or near real time, strategic view of the world. The CSP integrates all national level strategic information which includes detailed information on civil and political environments. Friendly military information is updated from the CONs and from national level intelligence assets.

In addition to containing all relevant strategic information, the CSN is intended to limit, but not eliminate, direct access to lower level information. By design, there is no tactical information resident in the CSP; however, specific tactical information can be accessed by request if needed. Operational information is necessarily tied into the network to keep the CSP accurate and continually updated. Although it is desirable to keep politicians and generals out of fighting holes, there may be instances when direct access to tactical information has immediate strategic value. As a result, designing out the commander’s ability to access available information within FORCEnet is not a desirable choice. Appropriate policies and business rules must be established, and followed, to ensure that commanders remain focused on their appropriate levels of war.

2. Common Operational Network (CON)

Similar to the CSN, the CON contains all operational level information for a given theater of operations. An important distinction between the two is that there may be multiple CONs active at any time. Each campaign will have its own CON configured by its operational level commander. Different CONs can share information laterally and do not need to work through the CSN. Operational Commanders have the discretion to determine what pieces of information reside on the network, and who may access each type of information. The Common Operational Picture, the COP, also resides on the CON. The COP contains all-source information, updated in real-time or near real-time, that is relevant to the operational level of war. This information may include force location and disposition, geography, supply routes, or significant cultural information depending on the mission and target country. Users may choose which pieces of the COP to be displayed at their local terminals, but the COP exists as a distinct object on the CON.

In addition to serving as the operational level storehouse of information, the CON also serves as the default common connection for lower echelon tactical units to share information and communicate. Direct communication between lateral and disparate units is not forbidden by this construct, but coordination through the CON is the standard.

3. Common Tactical Network (CTN)

The CTN is similar to the CON except that it is owned by the senior tactical commander for conducting an operation and contains relevant tactical information. Because levels of warfare often blur and the operational

and tactical commander can be the same, the operational commander can delegate the authority to establish and maintain a CTN or multiple CTNs to lower component commanders as necessary. An example of this is given in Chapter V. Also, as campaigns progress, the senior tactical commander may change as new or different units move into the theater which requires that ownership of the CTN will also change. The Common Tactical Picture (CTP) is contained on the CTN and contains all relevant tactical information. Specific differences between the CTP and COP are discussed in Chapter IV. For smaller combat operations and non-combat (Humanitarian Assistance, Peace Keeping, etc.) only one tactical commander may be in theater requiring a single CTN. More commonly, multiple CTNs will be established as assigned by the Operational Commander to divide responsibility and manage a large operation. CTNs have the ability to establish direct connections, share information, and collaborate as necessary to achieve operational goals.

Like the CON, the CTN contains all tactical information available and users have the ability to control what types of information are resident on their terminals. The CTN is fed by all Local Tactical Networks assigned to the tactical commander, as explained below, and is the lowest level of network responsible for integrating and aggregating information. In addition to serving as an information repository, the CTN also is the default communications hub for tactical units.

4. Local Tactical Network (LTN)

Each tactical echelon, to the lowest level practical, will have its own LTN. It is technologically feasible

today to have LTNs all the way down to the platoon or equivalent level. In the near future, it may be possible to have LTNs extending down to the fire team level. These networks serve two important functions. First they handle all information sharing and communications requirements within the appropriate unit. Secondly, LTNs are responsible for communications between LTNs and with the CTN as needed. LTNs do not normally feed the CON or CSN directly, but can when required.

Each unit owns its own LTN which is configured to meet the requirements for its level of command. For example, a platoon will maintain a separate network from the company LTN. Both the Company Commander and Platoon Commander can set policies regarding the platoon LTN, especially information sharing requirements. Likewise, the company LTN is separate from the battalion LTN, and this layering of LTNs continues until the next echelon owns the CTN for its area of responsibility. This network-of-networks construct not only allows for local control of information flow and information display, but it allows for LTNs to make direct links across command boundaries. Units from separate commands can connect laterally to share information in order to accomplish assigned missions without needing to traverse multiple layers of command organization. Lateral commanders, within guidelines established by their parent commands, can share information as necessary in order to facilitate self-synchronization.

5. Summary

Figure 5 shows an example of the four-tier connectivity. There may be multiple CONs active that are tied into the CSN at any given time. Likewise, there may

be multiple CTNs active. The default connections are standard communications pathways that follow chain of command lines. They exist under almost all conditions to transmit essential information within the command structure, but can be broken when appropriate to a mission. For example, if a platoon were attached to a different company the original default connections would be severed. Ad hoc connections are set up whenever units need to collaborate across command boundaries. These ad hoc connections may be temporary for simple intelligence reporting, or they may stay in place for the entire length of conflict depending on the situation and missions. The units in the figure are for illustrative purposes and are by no means meant to limit the scope of this structure to a standard infantry battalion. Supporting arms, other services, and other government agencies can easily be incorporated into the framework by adding the appropriate ad hoc connections.

C. ADAPTABLE COMMAND AND CONTROL (AC2)

For any vision of FORCEnet to be more than a military internet, it must be coupled with a command and control structure designed to take advantage of it. Network Centric Warfare was envisioned to flatten command organizations and free up lower level commanders to pursue opportunities on the battlefield. In order to accomplish this, a new way of defining command relationships and responsibilities is needed. Adaptable Command and Control (AC2) is one technique to marry command organizations with FORCEnet design and principles of NCW.

1. Distributed Decision Making Authority

Self-synchronization is discussed above, as well as some of the problems inherent in a self-synchronized force. The key component of self-synchronization is that forward

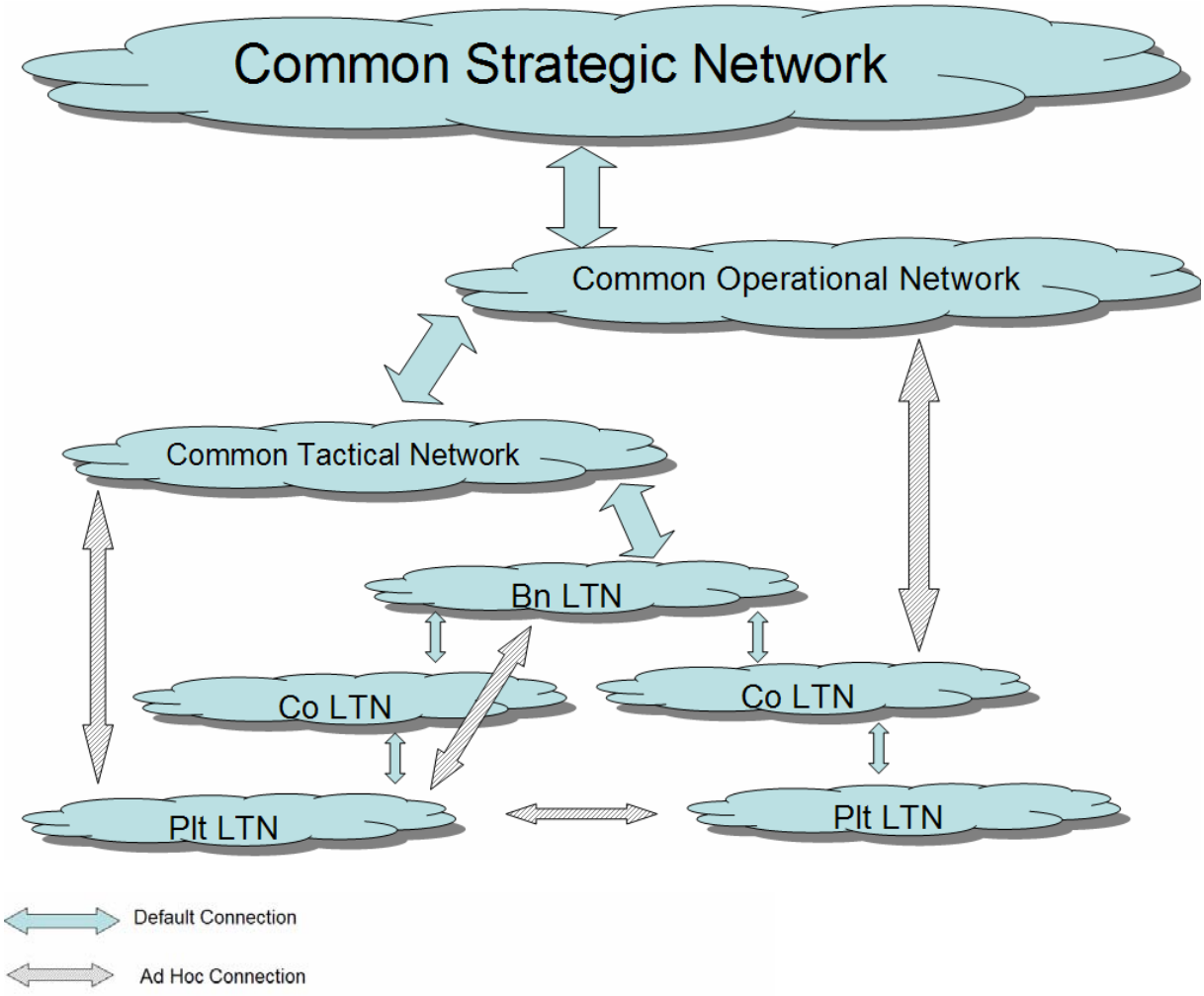

Figure 5. Four-tier Model

commanders can make battlefield decisions and take actions without waiting for orders or approval from higher command echelons.[50] Empowering lower level leaders to make decisions and take actions is not the same as distributing

[50] Arthur K. Cebrowski and John J. Gartska, "Network Centric Warfare: Its Origin and Future," *Proceedings of the U.S. Naval Institute,* January 1998

the command function. Commanders still retain their inherent responsibility, but delegate some authority to lower echelons as the situation dictates. By distributing the decision making authority during a conflict, units are free to take action while still maintaining ties to the larger command echelons. Higher level commanders orchestrate the action of their subordinate commanders by controlling their authority to act and through promulgating their commander's intent. The degree of authority to act granted a subordinate commander governs his ability to exploit battlefield opportunities, self-synchronize with other units, or take unplanned actions toward achieving specified goals.

During planning, commanders have the discretion to dictate which units have what level of authority to act. This process is similar to dedicating a main effort or supporting effort in a plan. The authority granted to a unit must clearly spell out what types of actions require clearance form higher authority. The default mode of operation should always be to give lower units the highest authority possible. Only missions that involve sensitive operations or high level coordination should be excluded. By granting subordinate leaders the authority to take action on the battlefield, the pace of the fight is greatly increased while still maintaining some control over the fight itself. The authority to make decisions and take actions on the battlefield can, and should, change with the character of the conflict. Oversight by higher level commanders is essential to ensure that forward units continue to operate as a cohesive force.

2. Multi-Level Control

No single method for controlling troops can ever work in all combat situations. Commanders need a way to selectively adjust the level of control they exert over their subordinates. Actions prior to open conflict are generally regarded as requiring tight control. Units are often in danger of escalating conflict prematurely or exposing friendly positions or movements by taking inappropriate actions. Conversely, during movement to contact or assaults on an objective, forward units need freedom to take actions on the battlefield. Multi-level control allows commanders to adjust the level of authority and responsibility for action across command echelons. Higher level commanders always have the option to step in and take control or push control to subordinate units as situations develop. By pushing and pulling control up and down the chain of command, commanders can ensure that their units have both the freedom of action necessary, and the cohesion to necessary to conduct military operations.

3. Lateral Collaboration

As explained above, the term self-synchronization has many definitions with slight variations in meaning. Here, a version of self-synchronization called lateral collaboration is used. Lateral collaboration is a method for coequal commanders or commanders from different higher commands to work together to decide on a course of action to accomplish an assigned or implied mission. Lateral collaboration also includes the tactical oversight by a higher echelon tactical commander of the decisions made by forward units. Small unit leaders and low level commanders will have the freedom to collaborate across organizational boundaries to take actions, while a higher echelon oversees

them to ensure that actions taken are in accordance and in support of larger tactical objectives. Each echelon of command is responsible for overseeing the action taken at lower levels and has the authority to override decisions made by lower level commanders. This version of self-synchronization does not distribute the function of command as Alberts and Hayes suggest, but provides a mechanism for commanders to exert their responsibility for subordinates through command oversight. In addition to oversight, commanders are responsible for arbitrating disagreements and conflicts that lower level commanders have.

a. Operational Commander

The operational commander is responsible for operational level issues while conducting campaigns. He sets the large mission objectives, sets the priorities of operational targets, handles logistics concerns, works with coalition partners and other government agencies, and sets high level policy for the conduct of the campaign. Since he is primarily concerned with operational issues, he should not be involved in tactical decisions made during the conflict unless decisions and actions taken have a direct conflict with operational objectives.

b. Lower Level Operational Commanders

Additional operational level commands may be established by the operational commander if needed. These additional command echelons are used for large or disbursed campaigns or whenever the operational environment is exceedingly complex. They have the discretion to laterally collaborate at their level within the guidelines set by the operational commander.

c. Tactical Commander

The tactical commander is the senior commander responsible for fighting the tactical battle in a given area. There may be multiple tactical commanders assigned by the operational commander for any operation. He is responsible for publishing mission orders, commander's intent, objective priorities, target priorities and precedence, levels of authority to act, and supported and supporting units. In addition, he orchestrates the overall tactical battle by overseeing lateral collaborative efforts of forward units. He arbitrates disagreements in resource allocation, courses of action, priorities of fire, and access to supporting arms. As the battle evolves, he pushes changes to objectives, targets, and courses of action to subordinate leaders.

d. Lower Level Tactical Commanders and Small Unit Leaders

Forward tactical units are generally the units engaged in actual combat. They also have the best immediate situational awareness and greatest need for freedom of action. Most lateral collaboration is done at the lowest levels, allowing small unit leaders and lower echelon tactical commanders the freedom to choose courses of action best suited to their immediate situation. During the collaboration process, coequal leaders will not always arrive at a common solution for a variety of reasons. If one assumes that both leaders have the same tactical picture by tapping into the CTP, they will not always agree on the proper course of action for their shared picture. Shared situational awareness is essential for lateral collaboration, but shared situational awareness does not guarantee success. Any two people will view their

situation from a different timeframe, perspective, scale and vantage point.[51] Also, coequal commanders will often have competing needs for supporting arms, non-organic assets, and logistics requirements. The higher echelon tactical commanders are responsible for arbitrating these disagreements.

D. SUMMARY

The four-tier model is what Barabasi called a scale free network in that its structure is constant regardless of what level of detail is viewed. Scale free topologies have some unique properties such as built in robustness and lack characteristic nodes[52]. The design is built upon a network of networks that can be assembled into whatever size is needed for any given operation. For this model to work it requires a command and control system design to work with the communications network. AC2 is such a command and control system.

In order for AC2 to be an effective means of controlling combat elements, commanders need to change what functions they perform and responsibilities they have. Table 1 summarizes the different responsibilities of each level of command for ensuring the success of an operation.

---

[51] CDR Al Elkins, Private Interview, May, 2004.

52 Albert-Laszlo Barabasi,. *Linked: How Everything Is Connected to Everything Else and What It Means for Business, Science, and Everyday Life.* (New York: Penguin Group, 2003).

Operational Commander	Lower Level Op. Cmdrs	Tactical Commanders	Small Unit Leaders
• Sets operational objective • Defines campaign goals • Determine mission priorities and precedence • Handles theater logistics • arbitrates operational lateral collaboration • Orchestrates operational battle	• Assigned as required • Laterally collaborate operational issues • Support operational level goals in assigned areas	• Define tactical objectives • Set target priorities and precedence • Allocate and re-allocate supporting assets • Provide commander's intent and mission orders • Arbitrate lateral collaboration • Orchestrate tactical battle	• Laterally collaborate to achieve tactical goals • Execute mission orders • Fight the actual battles

Table 1. Commander's Responsibilities.

IV. INFORMATION FLOW

A. RESIDENT INFORMATION ELEMENTS

Each tier of the four-tier model presented in Chapter III is intended to be fully configurable by the owner of the network. However, certain elements of information or types of information need to reside on these networks for them to be universally useful. Higher level networks will have larger amounts of archival information and processed intelligences while lower level networks will require more real time and unfiltered information. The elements covered here are not meant to be exhaustive or exclusive, and subject matter experts will eventually need to determine which pieces of information are critical and which are extraneous. It is important to remember that the owner of each network has the final say over what information resides on it and how it is shared. This discretion may be detailed in appropriate command policies so that, for example, a company commander has some say over what is on a subordinate platoon network.

1. Common Strategic Network

The Common Strategic Network is intended to be a permanent network maintained at the Department of Defense level in the continental United States. Because this network is terrestrially maintained with relatively unlimited access to power, data storage, and computing power, it can maintain a vast database, a large number of users, and fully integrate information across a spectrum of disciplines. The CSN is specifically designed to support the Strategic Level of war which is officially defined as

> The level of war at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) security objectives and guidance, and develops and uses national resources to accomplish these objectives. Activities at this level establish national and multinational support of tactical forces, and provide the means by which tactical successes are exploited to achieve strategic objectives.[53]

Because the strategic level of war deals with national level objectives, the information on the CSN needs to be of an appropriate scope to support national interest. Friendly and enemy force locations, dispositions, and logistics requirements are essential, but at the strategic level, it is vital that explanatory information be available for all force locations. A large view of a multiple tactical battle pictures is useless and unwieldy at the strategic level. For example, a blob of 1500 moving blue dots off the coast of a foreign country does not tell the strategic commander whether or not a key objective has been seized.

In addition to military information, locations and dispositions of other governments agencies are also necessary. The CSN is designed to handle top level integration and deconfliction of all national level assets, including CIA operatives, Ambassadors, Special Forces Teams, and NSA teams. In addition to integrating information across government agencies, the CSN houses an integrated intelligence picture culled from all source intelligence across the country. Raw intelligence as well as processed intelligence is integrated and analyzed to provide commanders a coherent strategic picture.

[53] JP 1-02, Department of Defense Dictionary of Military Terms.

2. Common Operational Network

The Common Operational Network is intended to be stood up and taken down as necessary wherever potential or existing conflicts exist. Multiple CONs may exist in any given theater of operations if multiple campaigns are active. An example would be that separate CONs are necessary to support campaigns in Iraq and Afghanistan. The CON is designed to support the operational level of war which is officially defined as

> The level of war at which campaigns and major operations are planned, conducted, and sustained to accomplish strategic objectives within theaters or areas of operations. Activities at this level link tactics and strategy by establishing operational objectives, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events. These activities imply a broader dimension of time or space than do tactics; they ensure the logistic and administrative support of tactical forces, and provide the means by which tactical successes are exploited to achieve strategic objectives.[54]

Because the operational level of war bridges strategy and tactics, the information resident on it must do the same. Operational actions happen at a faster tempo than strategic actions (usually, although historic counter examples exist), therefore information must be collected, analyzed, and displayed at a faster tempo than strategic information.

The increased tempo of operational level actions coupled with the transient nature of the CON implies that less processed intelligence will be available directly on the network. Detailed analysis of enemy culture, politics, and geography is resident on the CSN and can be requested

[54] Ibid.

as needed. Operational intelligence gathered, analyzed, and integrated from in theater assets makes up the bulk of enemy information resident on the network.

Friendly information is similar to that on the CSN, but is more granular and restricted to the local area of operations. Explanatory information is equally as important at the operational level as it is at the strategic. Exact locations of individual small units are not as important as the status of operational objectives and logistical support needs.

3. Common Tactical Network

The CTN is owned by the senior tactical commander, as described above, in any area of responsibility. The information resident on the network is intended to support the tactical level of war which is officially defined as:

> The level of war at which battles and engagements are planned and executed to accomplish military objectives assigned to tactical units or task forces. Activities at this level focus on the ordered arrangement and maneuver of combat elements in relation to each other and to the enemy to achieve combat objectives.[55]

At this level, real-time and positional information are much more important than at other levels. The explanatory information is still needed, but its importance is superceded by the location and disposition of units throughout the battlespace. Blobs of blue dots are preferable to mission status. Similarly, intelligence is often raw and posted before it can be properly analyzed so that commanders have access to the most current information. Standard tactical information covered in tactical orders is also resident here such as target lists,

[55] Ibid.

target priorities, mission objectives, fire control measures, etc. This information can be used to deconflict planning and execution of tactical missions throughout the operation.

4. Local Tactical Network

Because LTNs exist at different command echelons and in vastly different environments, from naval surface escorts to squad foot patrols, the information on each network will vary greatly. Each LTN will primarily contain a subset of the information contained on the CTN amplified with whatever local information is deemed important by the networks owner.

B. INFORMATION EXCHANGES

1. Standard Exchanges

Information exchanges between networks can be of two general types: standard and on-request. Standard exchanges are those called for by existing policy. Information that is routinely shared by units is done through a standard exchange. Often these are done automatically and follow chain of command lines. For example, a position report (posrep) from a forward unit to its next higher command is a standard exchange. This information is automatically sent to the next higher command echelon, for example from platoon to company, aggregated with existing friendly locations, and automatically sent to the next echelon. These exchanges are covered by existing doctrine and unit Standing Operating Procedures and include position reports, situation reports, SALUTE reports (enemy location and disposition), and any other standard reports.

In addition to standard reporting, certain tactical and operational requests are considered standard exchanges.

Calls for fire (CFF), joint tactical air requests (JTAR), assault support requests (ASR), logistics support requests (LSR), naval surface fire support requests (NSFS), and any other common battlefield requests are handled as standard exchanges. The information is automatically sent to the appropriate units identified by doctrine. The individual addressees are imbedded in the request type, so that a call for fire, for example, is routed to the appropriate artillery battery, the fire direction center, the fire support coordination center, as well as higher command echelons. This information is also immediately posted to the common tactical network so that the requesting unit, supporting unit, nature of request, and target can all quickly be identified and fires can be integrated and airspace deconflicted.

Standard exchanges are intended to move along doctrinal command lines in accordance with established procedures. Lateral, or coequal, units can set up standard exchange criteria when they are brought together to conduct a mission or perform tasks. The intent of standard exchanges is to streamline the communications process so that all parties know what information they are expected to send and what information they can expect to receive during each phase of the battle. These standard exchanges also help prevent extraneous communications exchanges so that an engaged unit is not receiving irrelevant information.

2. On-Request Exchanges

While standard exchanges follow doctrinal command lines, on-request exchanges are ad hoc in nature. Units at any echelon request information by type, sending unit, location, or any other parameter that the appropriate

commander deems important. An operational commander who has a particular interest in a tactical sensor can make a request to receive the raw data from that sensor. Similarly, a strike aircraft flight lead can request any information regarding RADAR detection in a certain area be immediately forwarded to his aircraft for the duration of his mission. Standard exchanges are designed to streamline information exchanges and minimize extraneous information; conversely, on-request exchanges are meant to be flexible and fill any gaps that the standard exchanges do not. On-request exchanges are intended to be specific in nature and cover limited time scales, but they may be active for the duration of conflict if necessary.

C. EXAMPLE

Figure 6 shows a nominal command structure for a sample organization with both organic (owned) and non-organic (supporting) assets. At the top is the Tactical Commander (TC) who owns the Common Tactical Network (CTN) and all assets in this example. For purposes of this example, the CTP is maintained at the TC node. Directly under the Common Commander is an intelligence and operations asset (Intel) which analyzes, integrates, and otherwise processes raw data. This asset updates processed information to the CTP. Subordinate to the TC are two (or more) Higher Headquarters echelons (HHQ). The exact organization the HHQ represents is irrelevant and could be anything from an infantry company to an expeditionary force. This model scales easily with command levels added as appropriate. Subordinate to each HHQ are several forward combat units (Unit). In addition to the named units, there are multiple sensors (Sensor) and supporting arms (SA). Like the HHQ, the exact nature of the sensors

and supporting arms is irrelevant. A sensor organic to a forward Unit has been tasked to look at a named area of interest (NAI). A target (Tgt) is active on the battlefield undetected by any sensors or units.

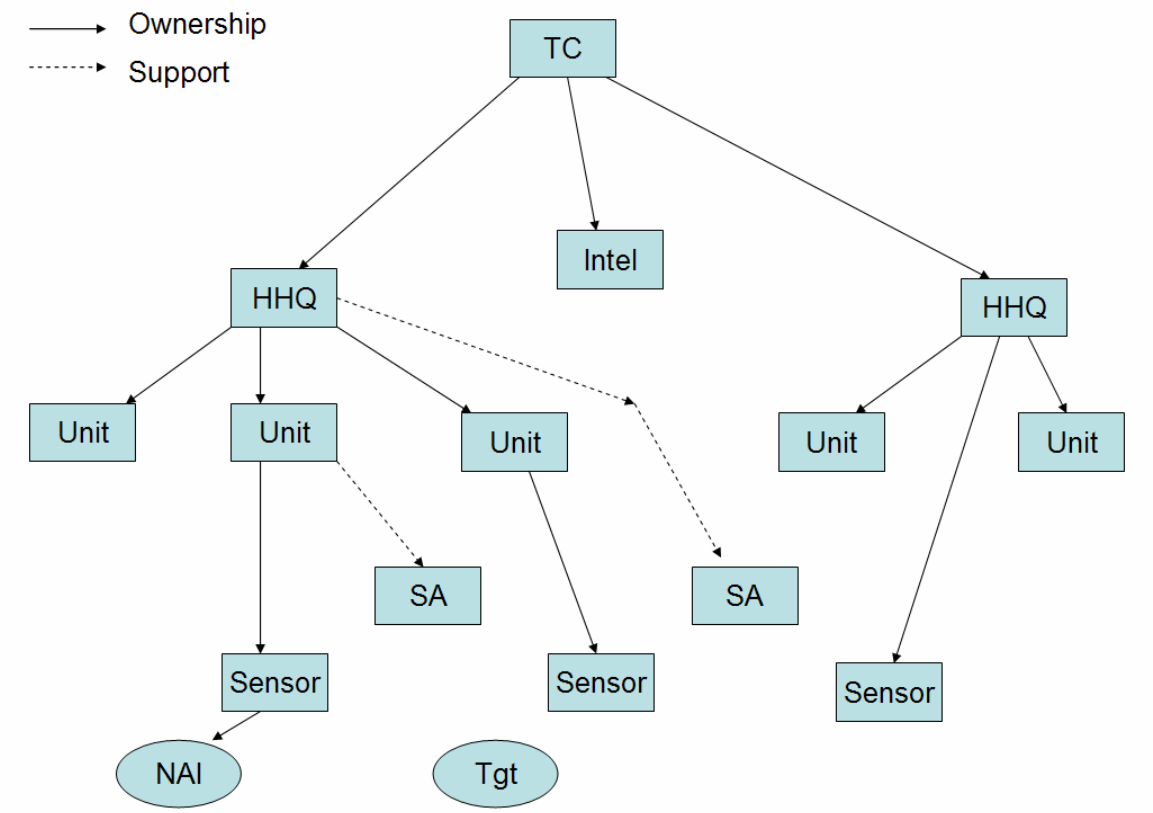

Figure 6. Command Structure Example

The sensor collects information from the NAI and automatically transmits it back to its tasking unit and directly to the Intel unit for analysis and integration. Because this information is a standard intelligence report, it is treated as a standard exchange and is automatically forwarded from the Unit to its HHQ who aggregates it and passes it back to the TC. The TC automatically aggregates this information, updates the information to the CTP, and forwards it with associated aggregate information to the

Intel unit which integrates and analyzes the information, updates the CTP with the processed information, and pushes the update back to the HHQ units. The same information is updated to the CTP twice. The raw data that has been aggregated and unverified is posted immediately so that all units have access to it. The data is tagged (see Metadata above) to identify that it is unprocessed. Once the Intel unit has verified and integrated the information, the latest version is updated to the CTP and the tag adjusted as necessary. The HHQ also sends the raw information to a SA asset that is in direct support of the HHQ. From the TC, all information is forwarded to the operational commander to update the COP. Figure 7 shows the standard exchanges up to the TC level.

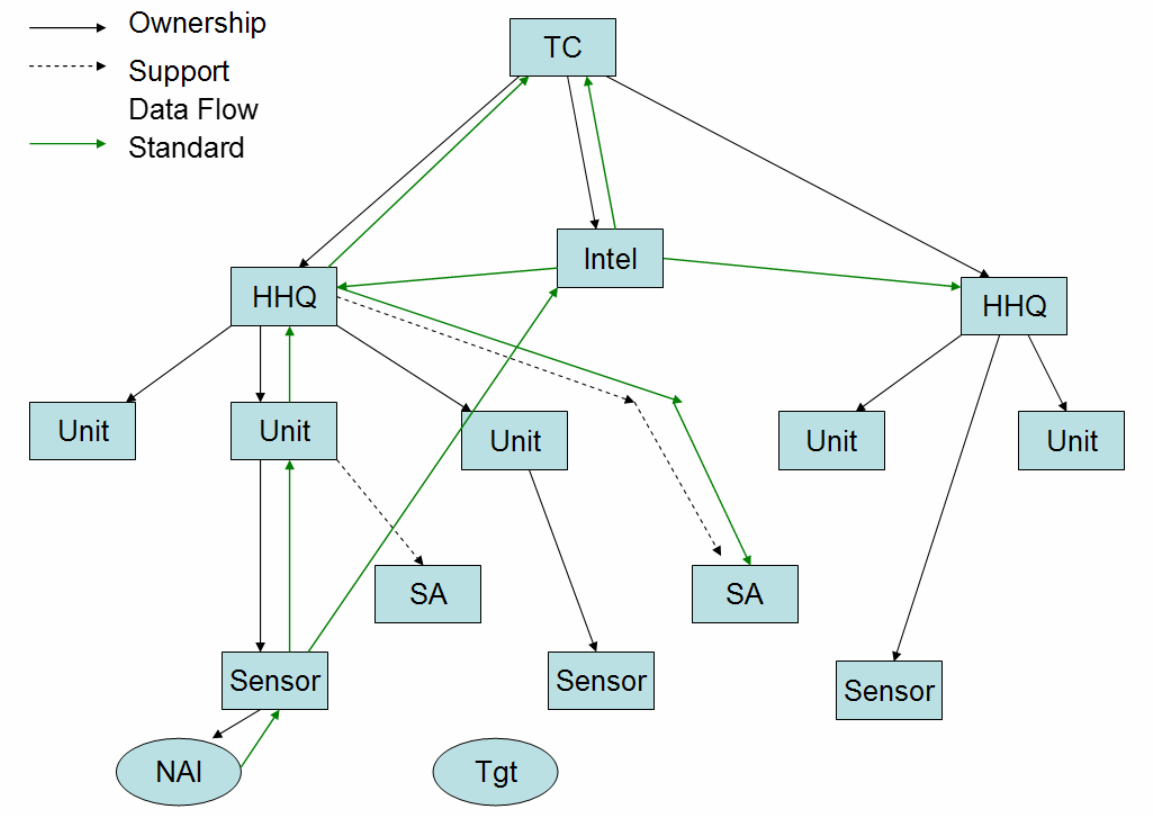

Figure 7. Standard Exchanges

In addition to the standard exchanges shown in Figure 7, on-request exchanges can be made as needed by units in the area of responsibility. Figure 8 shows an example of possible on-request exchanges. Here, lateral Units under the same HHQ request to receive the raw intelligence information directly from the sensor. Also, lateral Units under a different HHQ have requested the aggregated data from the tasking Unit, and the lateral HHQ is receiving aggregated information from the tasking HHQ. The SA asset in direct support of the tasking unit is also receiving raw information from the sensor, as is the TC. These exchanges are requested for a specific period of time, and may be active requests throughout the conduct of operations or only for a specific incident. Even if Units and HHQ do not request raw data from the sensor, they will get the information provided by the sensor once it has been integrated into the CTP and sent back down to these elements.

Figure 9 shows an untasked sensor receiving a signal from a pop-up target. The sensor immediately reports back to its organic unit and may report raw data to other elements in the area. The sensor can have the ability to process the sensed data and determine what units need the information. For example, a sensor which identifies an enemy air defense asset would immediately send the information to all aircraft in the area. Likewise, a sensor that sees vehicles moving toward a friendly Unit’s position can send the information to that unit. These exchanges are similar to on-request exchanges except that they are pushed by the data producing element to units that need the information.

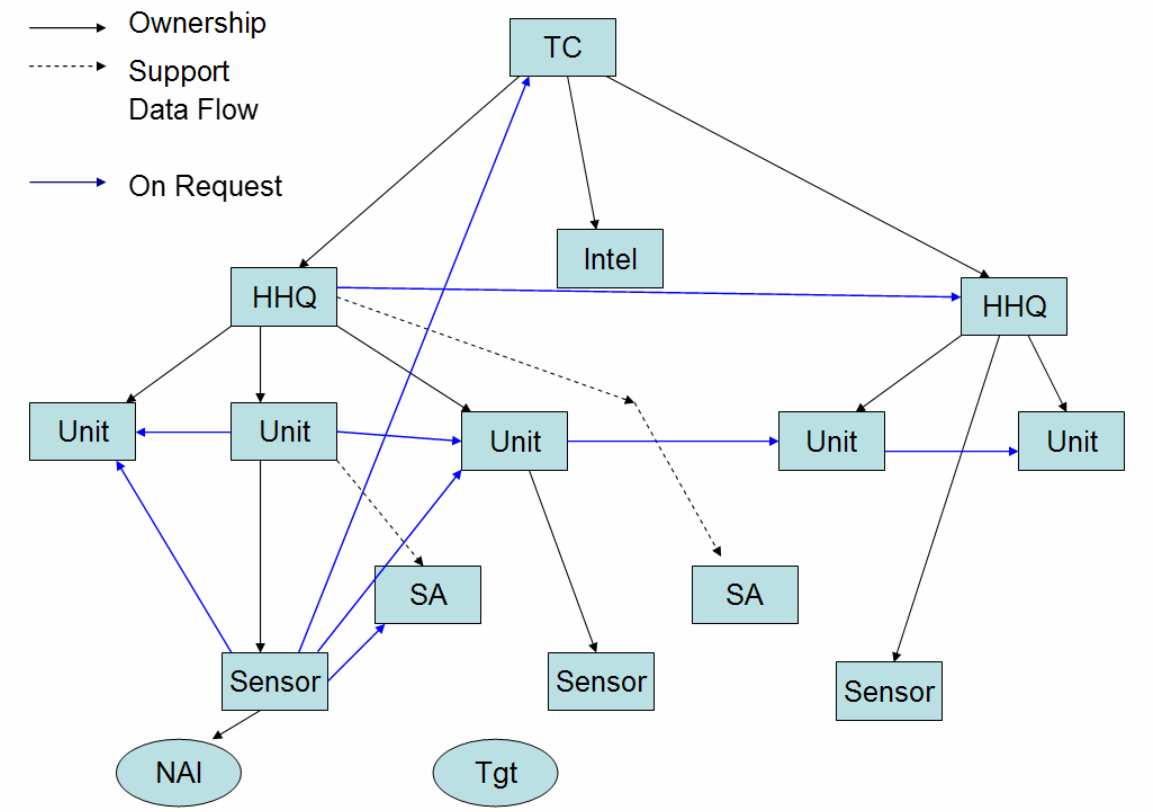

Figure 8. On-request Exchanges

The network must also be able to identify when an element is no longer on the network and adjust its data flow accordingly. For example, the sensor above is reporting back to its tasking Unit which suddenly drops off of the network. The sensor recognizes that the Unit is gone and starts reporting back to the next command echelon, in this case the HHQ.

D. SUMMARY

The above example shows one way that information can be exchanged within the four-tier model. Standard exchanges provide a set of default connections that mirror standard military organizations. They allow commanders to have existing links with senior and subordinate units. On-

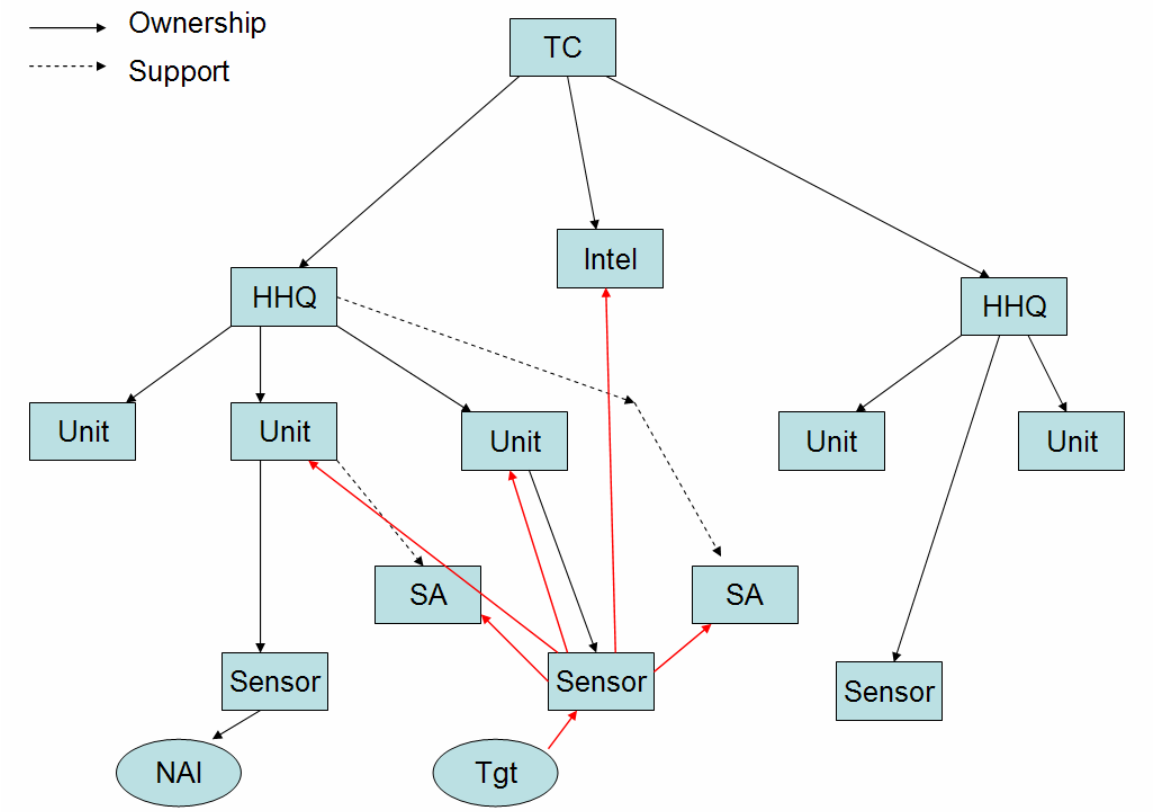

Figure 9. Pop Up Target

request exchanges provide flexibility to the network so that units can get the information they need from non-organic assets. These exchanges facilitate conducting Network Centric Warfare by providing the robust communications backbone and a system for exploiting available information. Adaptable Command and Control takes advantage of the network's ability to connect co-equal and disparate units by providing a command organization capable of self-synchronization. Chapter V further explores these ideas with a hypothetical example involving multiple tactical missions in support of operational and strategic goals.

V. SCENARIO

A. CAVEAT

The below scenario is designed to give a realistic example of how the four-tier model for the FORCEnet network could be employed. The political situation outlined below is only important in that it sets the stage for the action. Likewise, strategic, operational, and tactical decisions are made to provide examples of how the system can be used. Specific details of force structure are unimportant; however, current Expeditionary Strike Group (ESG) and Carrier Strike Group (CSG) compositions are used. Lastly, certain technological specifics are intentionally overlooked such as input/output devices, software tools, and communication systems because their details are not important to the discussion. It is assumed that information can be put into the system, exchanged between users, and displayed in a useful manner. What is important to the scenario is how information moves between users and how the information flow affects the way the operation is conducted.

B. BACKGROUD

The coastal nation of S___ bordering the international shipping lanes of the Straits of M___ has been largely overrun by insurgents. The legitimate government still has control over most of the capital and its international airport and shipping port, but has lost control over all other areas including the major city of J___ and its international airport. Insurgents have threatened to close international commercial shipping lanes if the legitimate government does not capitulate soon. Shutting down the

straits, even temporarily, will have an immediate negative impact on regional countries. If the straits are closed for any significant length of time, global commerce will be greatly impacted and many economies will suffer. Piracy in the straits has been a minor problem for decades, but now that the coastal ports are under insurgent control commercial vessels are regularly attacked and plundered. The US government has determined that reopening the straits to commercial traffic is a top strategic priority, followed closely by the reestablishment of the legitimate government within the country of S___.

The closest forces to the conflict are a full Expeditionary Strike Group (ESG) and a Carrier Strike Group (CSG). Also, a neighbor country has offered to send a company-sized contingent of Royal Marines and a squadron of naval patrol craft to aid in the operations. A US Army brigade is put on alert and can be in theater within 96 hours. The Regional Combatant Commander has designated the ESG commander as the interim Joint Force Commander for the early phases of the operation. The CSG is designated a supporting unit and is in direct support of the ESG for the early phases of the operation. All units expect a Standing Joint Force Headquarters (SJFHQ) to take over the operation once additional assets have been brought into theater, including the Army brigade.

C. OPERATIONAL ACTIONS

The ESG Commander divides the operation into three Operational Mission Areas each with a separate Tactical Commander who is ordered to stand up a Common Tactical Network. The division of responsibility is by mission area. Geographical areas occupied and supporting assets

required for each mission may overlap. Each Tactical Commander is responsible for resolving any potential conflicts.

1. Reinforce the Capital

The ESG Commander has assigned the coalition Royal Marines to execute an unopposed landing to reinforce the legitimate government's security in the capital. They are reinforced with the MEU's organic HUMINT Exploitation Team (HET), Military Police units and any necessary public affairs or civil affairs assets. The Combat Service Support Element Commander is assigned as the Tactical Commander and stands up the CTN. The coalition Royal Marines and the security forces of the legitimate government are granted access to the CTN so that they can share relevant tactical information. Their access is restricted to types of information that the Tactical Commander sees as relevant, and they do not have full access to the entire FORCEnet network. The level of access to the CTN granted to the coalition commanders can be adjusted as necessary by the Tactical Commander while access to information at the CON is controlled by the ESG Commander.

2. Protect Commercial Shipping

The CSG Commander is given the task of protecting commercial shipping in the straits. He establishes a CTN and sets his tactical goals. Escort plans are established, strikes on pirate vessels are conducted, and Theater Ballistic Missile Defense is set up. Many of his strike assets and Naval Surface Fire Support (NSFS) assets will be tasked to support operations ashore. The CSG Commander is responsible for deconflicting these requests with his own needs while performing escort and anti-piracy operations.

Because re-establishing international commerce has been set as a higher strategic goal than the reestablishment of the legitimate government, the CSG commander has priority of use for these assets.

3. Restore Legitimate Government Authority

The ESG Commander designated the MEU Commander as the Tactical Commander responsible for restoration of the legitimate government. The MEU Commander stands up his CTN and prepares to defeat the insurgency ashore. He establishes the following tactical goals to achieve this mission: 1) neutralize insurgent ADA capability, 2) execute an airfield seizure at the city of J___, and 3) search out and defeat the insurgent forces in the countryside. Although his organic supporting assets have been reduced by the other operations in the area, he is laterally tied in to both other CTNs and can quickly share information as well as request assets.

4. Lateral Collaboration

Three concurrent operations are drawing assets from the ESG and CSG. The ESG commander has divided responsibilities among his subordinates, set his priorities, and issued mission orders. The three tactical commanders assigned have the authority to laterally collaborate so that they can dynamically share assets. The final authority to apportion, allocate, and re-allocate assets rests with the ESG commander, but each tactical commander can collaborate with his peers and agree on appropriate courses of action without additional approval from higher. As long as the co-equal tactical commanders can agree on courses of action that meet operational requirements, no additional approval from the ESG commander is needed.

Figure 10 shows a graphical view of how forces relevant to the example are divided and which commander controls each network. Default connections are shown between command echelons and follow chain of command lines. Ad hoc connections discussed in the example are also shown. It is important to note that additional ad hoc connections can be made when necessary and the ad hoc connections shown should not be viewed as the only possible connections. The connection from the CON to the CSN is also not shown but exists.

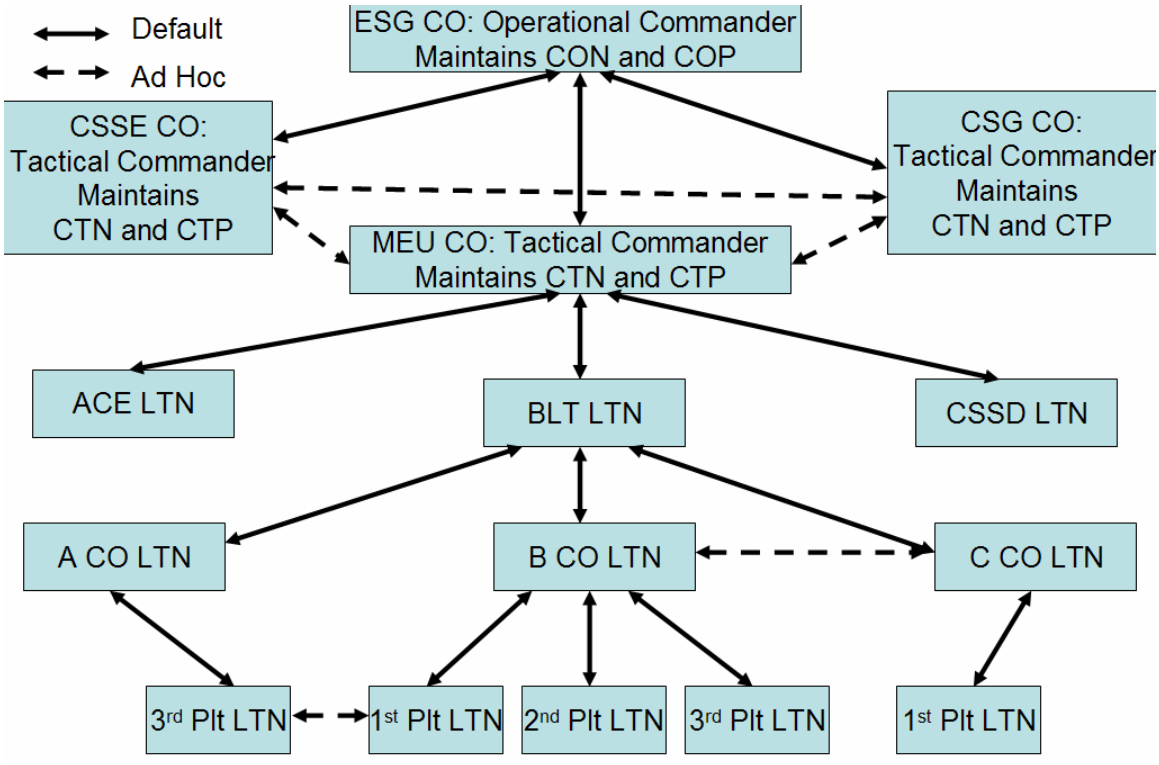

Figure 10. Force Breakdown

D. TACTICAL ACTIONS

While escort, anti-piracy, and security missions are being executed by the other Tactical Commanders, the MEU Commander prepares his assault on the city of J___. He

deploys his organic reconnaissance assets and taps into the COP to get information from national level intelligence sources. Planning begins as the CTP is populated with available data. Any HUMINT gathered in the capital concerning force disposition and position of ADA assets is routed to the MEU CTP via on-request information exchanges as is any relevant information gathered by other operating forces in the area.

1. Neutralization of ADA

A limited number of SA-X systems are controlled by the insurgents and are capable of prohibitively interfering with friendly air in the vicinity of J___. A sensor has identified the location of one SA-X and passes the location to the COP. The raw data from the sensor is automatically routed to the CTP via an on-request exchange. ESG analysts confirm the location with other intelligence reports and update the original report. The updated data is filtered down to the CTP via a standard exchange and is further disseminated by the same method. A reconnaissance unit in the area receives the update and is able to move into a position to observe the SA-X position.

The reconnaissance team places a call for fire which is routed to the Supporting Arms Coordination Center aboard the ESG and is filled with a cruise missile from a CSG shooter. The request, along with trajectory information and intended target is immediately forwarded to each CTN to identify potential conflicts. The flight corridor is identified and deconflicted with friendly air assets from all three mission areas. Once the missile is launched, it notifies the reconnaissance team that it is in the air and requests a target update. The SA-X battery has not moved,

so no updated location information is required. After impact the reconnaissance team files a battle damage assessment (BDA) report which is automatically disseminated via standard request up the chain of command to the CTP and COP. The report is integrated at the COP and the updated air picture is automatically forwarded to all air units.

This evolution required four distinct pieces of information: the original target location, the call for fire, the launch of the missile, and the BDA report. Each of these reports was sent from the source to one other person. Once received, the network identified the type of information and, using appropriate rules for standard and on-request exchanges, disseminated the information to all relevant personnel. The information was quickly shared by all players with almost no need to manually transmit the data.

2. Airfield Seizure

The bulk of the assault force is on the ground, and they are successfully pushing the insurgents off the air field. The MEU Commander is monitoring the CTP which shows where all forces should be as well as where they have most recently reported in. The enemy picture is still fuzzy as he and his staff wade through conflicting reports from a variety of sources. Even with modern sensors and computer-aided information analysis, the fog of war is not completely lifted. However he does have a clear view of where his forces are and how far from the plan they have deviated. So far things are going relatively smoothly and he continues to monitor for changes.

Third Platoon, Alpha Company has just pushed a group of insurgents out of their defense and recognizes Third

Platoon can destroy or capture the unit if he immediately pursues. The insurgent direction of retreat takes them across the Company boundary into First Platoon, Bravo Company's zone of control. Not wanting to lose the opportunity, Third Platoon Commander initiates an ad hoc connection with First Platoon and begins collaboration. First Platoon is able to readjust their position to set up a blocking position in support of Third Platoon's pursuit. Third Platoon pushes the enemy into First Platoon's sector of fire and quickly eliminates the remaining threat.

When Third and First Platoons agreed on their course of action, they each sent their intentions (intended direction of movement, new defensive positions, etc.) up the chain of command via a standard exchange. This information was automatically distributed to company, battalion, and MEU headquarters, as well as the fire direction center (FDC) and supporting arms coordination center (SACC) for supporting arms deconfliction.

Alpha Company was initially designated the main effort and is engaged in moderate fighting to clear airfield buildings. The Alpha Company forward air controller (FAC) has control of fires and has several sections of rotary wing close air support (RWCAS) available. Across the airfield Bravo Company's left flank has routed an enemy position and is giving pursuit. The Bravo Company Commander pushes his Third Platoon forces forward of their assigned zone in pursuit of the enemy. With his First Platoon involved in cutting off the retreat of one group of forces and his third platoon pursuing a separate group, the Bravo Company Commander recognizes that his forces are being stretched too thin to defend the access road he has

been assigned. He initiates an ad hoc connection with the reserve company, Charlie, for some additional support in his sector until he can reconsolidate. Charlie agrees to commit a platoon and both commanders report their intentions.

The MEU CO sees the incoming changes and recognizes a potential disaster. Bravo Company, attempting to exploit their advantage, is splitting his forces too much. One platoon is chasing the enemy beyond the rest of the forces' ability to support and now the Bravo Company commander is attempting to commit a portion of the reserve. To compound matters, The MEU CO just received an unconfirmed intelligence report that vehicles have been spotted moving down the access road that Bravo is supposed to be supporting. He decides to override the lateral collaboration between Bravo and Charlie and order Bravo to reconsolidate now on his assigned position. He also relocated the RWCAS assets from Alpha Company to Bravo to deal with the upcoming conflict. He recognizes that pulling assets away from Alpha may slow their advance, but if the vehicles overrun Bravo, they may lose the airfield.

The MEU CO's orders are immediately forwarded down the chain and all units receive the update to the plan. Bravo Company pulls back Third Platoon from their pursuit and quickly readjusts First Platoon to their original position. With Bravo Company reinforced with the RWCAS, the reserve can be held until the MEU CO needs to commit them.

As each smaller unit laterally collaborates to achieve assigned specific assigned missions, the forces can start to drift apart and lose coherency. The ability of the four-tier model to automatically forward information to all

concerned players allows higher echelon tactical commanders to see the big picture while the lower level commanders focus on the details. If the force starts to drift so far apart that it is in danger of losing coherency, the higher echelon commanders have the ability to recognize it and take action. By overriding lateral collaboration at the platoon level, the MEU CO was able to ensure that his units were in position to repel the enemy counterattack. Also, the MEU CO is able to dynamically reallocate assets (the RWCAS) so that the forces that need them right now can get them. Had Bravo Company attempted to laterally collaborate with Alpha to get the RWCAS, his request may have been denied by the Alpha Company Commander who was actively using the RWCAS and had priority. The MEU CO was able to readjust priorities, re-allocate assets, and ensure the coherency of his unit during the conflict.

E. ADVANTAGES OF THE FOUR-TIER MODEL

1. Advantages over Current Model

Showing the definitive advantage of a networked force over a non-networked force is beyond the scope of this paper. Several authors have attempted to quantitatively show the advantage of a networked force with varying results. The bibliography and reference sections contains list of several books and papers that attempt to back up this claim. A few qualitative advantages are listed below.

a. Lateral Collaboration

The forces presented above laterally collaborated at many levels. The Tactical Commanders were able to set up ad hoc connections between their CTNs so that they could laterally collaborate when necessary. When the request for a cruise missile came in from the reconnaissance team, the MEU CO was able to laterally collaborate with the CSG CO

for a shooting asset and for deconfliction of the flight path. Platoons and companies could directly connect their LTNs to laterally collaborate as needed. Platoons from different companies could connect directly, agree on a course of action, and automatically update their intentions up the chain of command. There was no requirement for either company commander or the battalion commander to directly get involved with the collaboration, but they each were automatically informed about the new course of action and could take action as necessary. Because higher echelon commanders retain command oversight, the MEU CO was able to step in and prevent Bravo Company's action from tipping into chaos. By reigning in the authority to act by the platoon commanders, the MEU CO was able to maintain coherency of his forces.

b. Speed of Command

Alberts, Gartska and Stein define speed of command as "the time it takes to recognize and understand a situation (or change in the situation), identify and assess options, select an appropriate course of action, and translate in to actionable orders."[56] The four-tier model offers several ways to increase speed of command.

The CTP is updated in real time and each user has the option to design individual views. The CTP also contains both raw and processed data so that users have access to the most recent and relevant information at all times. The MEU Commander was able to quickly recognize that Bravo Company was drifting into separate units unable to defend the access road. Likewise the Third Platoon

[56] David S. Alberts, John J. Gartska, and Frederick P. Stein, *Network Centric Warfare*. (Washington: Department of Defense, 1999), 163.

Commander could quickly see that the insurgents he routed were retreating into another company's sector.

Having access to the original plan and the current disposition of friendly forces allowed each commander to quickly identify potential courses of action. Since all players are operating from the same picture, lateral collaboration toward a new course of action can be made quickly. Also, once orders are issued, they can be easily understood and quickly disseminated.

2. Four-Tier Model and NCW

The four-tier model for an information topology of FORCEnet takes advantage of the potential power of NCW. Alberts, Gartska, and Stein say that the power of NCW is achieved by "linking together – or networking – battlespace entities."[57] The four-tier model allows all players to have a potential direct connection without the need for open channels between every node. The network of networks structure also allows each command echelon to establish a unique network tailored to its needs without requiring the hardware and software overhead of managing all users on one system. Because each local network is directly connected to several other networks, the design has built-in redundancy and robustness of communication. No single node can ever be a critical node that shuts down the network, and users who are separated from the rest of the network can still function with data stored at their location.

F. SUMMARY

The above scenario illustrates how information would move through the four-tier network. The ability to laterally collaborate is allowed by direct ad hoc

[57] Ibid., 93.

connections between networks, and command oversight prevents the collaborating units from drifting into chaos. Although an example of swarming forces was not used, the same processes that allow lateral collaboration will also provide a swarming capability. In Chapter II, Alberts' and Hayes' assumptions for self-synchronization were listed as:

- Clear and consistent understanding of command intent;
- High quality information and shared situational awareness;
- Competence at all levels of the force; and
- Trust in the information, subordinates, superiors, peers, and equipment.[58]

The second assumption is the only one that can be solved with a technological solution, and is met by the four-tier model. Clear understanding of command intent can only take place in the mind. The best any information system can do is to provide clear information in the proper format and context, and this is facilitated by the four-tier model. The last two assumptions can only be accomplished through training and effective use of the system.

[58] David S. Alberts and Richard E. Hayes, *Power to the Edge*. (Washington: Department of Defense, 2003), 27.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

The four-tier model presented above was designed to define an information topology that employs the principles of Network Centric Warfare. The network-of-networks design allows for an easily scalable structure built from interchangeable pieces. Every layer of the network can be viewed as a collection of nodes with each node being a distinct network itself. This layering of networks eliminates any critical nodes upon which the entire design relies. This design also provides a degree of autonomy for each network by allowing the owner of each network the authority to configure it to his needs. The four-tier model also provides a set of default communications pathways with the ability for user to make direct connections when necessary.

For this type of system to work, it requires a command and control philosophy designed to maximize the flexibility and responsiveness of a Network Centric force. Adaptable Command and Control (AC2) provides one method for doing this. AC2 seeks to maximize the flexibility of military organizations by allowing lateral collaboration at the edge of the organization. In addition, AC2 retains the traditional command roles that some have attempted to remove from self-synchronizing units. With AC2, senior commanders have the specific responsibility of overseeing lateral collaboration to ensure that subordinates are acting in concert with stated goals. AC2 also provides a set of rules and criteria that units can train to and

understand so that forces attempting to conduct NCW will have a common foundation on which to operate.

The four-tier model has one other important property; it is testable. This design is a specific instantiation of a FORCEnet information topology that can be modeled, simulated, and tested. Future modeling and simulation will aid developers in identifying and correcting shortfalls in the design and fielding of a superior product in the end. Before this type of design can be implemented, many technological concerns need to be addressed. Some are addressed specifically below, and others were highlighted in Chapter II.

B. TECHNOLOGY CONSIDERATIONS

1. Ad Hoc Networking

Ad hoc networking is defined as "a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or standard support services."[59] The four-tier model relies heavily on ad hoc networking to connect forward units into the network. Many companies have fielded local ad hoc networking capabilities, but no networks have been fielded on the scale of the FORCEnet network. Additional advances in routing protocols, pathway identification, and addressing algorithms still need to be developed and tested before the four-tier model can be fielded. In addition, more advanced computing and data transmission systems are needed to field this network.

[59] David B. Johnson, "Routing in Ad Hoc Networks of Mobile Hosts," *Proceedings of the IEEE Workshop on Mobile Ad Hoc Computing Systems and Applications,* December 1994.

a. Storage and Processing

The four-tier model presented in Chapter III assumes the availability of small, powerful computer processors and data storage components for forward units. Units deployed at permanent or semi-permanent installations or on ships will have the potential to access adequate computing and power sources. Some information technology companies and universities have made promising advances in the area of small-scale, powerful computing and storage systems (see Chapter II, Section C), but no products have been developed to meet the needs of the four-tier model. Forward units need to have a man-portable system that can receive datalink communications, process data, display information in a usable format, determine if data meets the requirement of a standard or on-request information exchange, and transmit the data as appropriate. In order to reduce bandwidth requirements, more information needs to be stored and processed at the forward edges of the network so that less raw data needs to be transmitted. The ability to store necessary information forward, such as copies of the CTP or mission orders, allows units to continue to operate effectively when denied access to the network.

b. Transmission

The amount of data exchanged between two wireless hosts is limited by a number of factors. The most obvious is bandwidth, which limits the number of actual bits that can be exchanged[60]. The amount of useful bits of information is far less than the number of bits transmitted. Forward error correction, such as Hamming codes or turbo codes, sends redundant bits to compensate

[60] Bernard Sklar, *Digital Communication: Fundamental and Applications (2nd Edition).* (Upper Saddle River, New Jersey: Prentice Hall PTR, 2001), 42-49

for poor signal connectivity and is required whenever data is sent over a wireless connection[61]. Stronger transmitting power can reduce the requirements for forward error correction but can never eliminate it. Additionally, transmission power is a drain on portable power sources which can be expected to be at a premium for forward units. Data compression algorithms can squeeze more useful information into fewer bits of data. These algorithms vary in their performance and usefulness,[62] and no universal standards have been accepted although several protocols are used commercially. Wireless bandwidth expansion, transmission power, and data compression standards need to be designed into the FORCEnet network in order to enable ad hoc networking in field environments.

2. Data Fusion and Analysis

The four-tier model rests on an assumption that all data residing on the network is of a commonly readable form. In order for a common data format to exist, several problems need to be resolved by appropriate subject matter experts. Many of these problems are beyond the scope of this work, but a few are presented here. First, the system needs to have a mechanism for identifying redundancies in data. If two units report the same, or nearly same, information, the system needs to be able to recognize and resolve the condition without simply double reporting the data. This is not a trivial problem because two reports that are nearly identical may be reports on separate events, the same event, or the same event moving in time. When reports are fused, the time nature of the reporting as

[61] Ibid., 305-374.

[62] See http://www.DataCompression.info for more information on data compression. Last accessed September 2004.

well as the reliability of the source need to be kept intact so that analysts can determine which reports are relevant and which no longer apply.

A second problem is determining the appropriate mix of human and autonomous analysts that should be involved in analyzing information. Some sensors already rely heavily on computer-aided analysis. For example, a radar system that rejects clutter and an infrared seeker which rejects flares both rely on algorithms to determine what is a potential target and what is not. It is not difficult to conceive of advanced computer-aided systems in the near future that can make similar determinations quickly on the battlefield. This capability has the potential to be extremely advantageous or catastrophic depending on the environment in which it operates. The mix of humans and automatic analysis aids needs to be determined clearly when these aids become available in order to ensure that the maximum benefit can be gained.

C. RECOMMENDATIONS FOR FUTURE WORK

1. Modeling and Simulation

Before any project of this magnitude can be developed, appropriate models need to be built to show that the basic design will work. The four-tier model lends itself to modeling partially because its scale-free nature fits an understood and developing field of network theory. Also, the design has well-defined rules that can be designed into a model.

AC2 needs to be further explored to determine if the lateral collaboration and command oversight construct is sufficient to provide flexibility and coherency of forces.

This design could be easily wargamed as a start and eventually worked into a field exercise at a small scale.

LIST OF REFERENCES

Alberts, David. S., Gartska, John. J., & Stein, Frederick. P. (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority(2nd ed.).* Washington, Department of Defense Command and Control Research Program.

Alberts, David. S., & Hayes, Richard. E. (2003). *Power to the Edge: Command… Control… in the Information Age.* Washington, Department of Defense Command and Control Research Program.

Barabasi, Albert-Laszlo. (2003). *Linked: How Everything Is Connected to Everything Else and What It Means for Business, Science, and Everyday Life.* New York, Peguin Group

Berkowitz, Bruce. (2003). *The New Face of War: How War Will be Fought in the 21st Century.* New York, The Free Press.

Cebrowski, Arthur K. and John J. Gartska, "Network Centric Warfare: Its Origin and Future," *Proceedings of the U.S. Naval Institute,* January 1998.

Chief of Naval Operations Strategic Studies Group XXI (2002). *Accelerating FORCEnet – Winning in the Information Age.*

Clark, Vern, "Sea Power 21," *Proceedings of the U.S. Naval Institute,* October 2002.

Denning, Dorothy E.(1999). *Information Warfare Security.* New York, ACM Press.

Department of the Navy Publication (2003). *Naval Transformation Roadmap 2003: Assured Access & Power Projection…From the Sea (Sec D.).* Washington, Department of the Navy.

Department of Defense Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms.* Washington, Department of Defense.

Elkins, Al, Private interview with the author, May, 2004.

Futures Center, Training and Doctrine Command, United States Army, "LANDWARNET Brief," February 2004.

Futures Department, Marine Corps Combat Development Command (MCCDC), Private Communication, 17 March, 2004.

Gershenfeld, Neil, Director Center for Bits and Atoms at MIT. Private Communication. January, 2004

HP Labs, Series of Presentations given March, 2004.

Johnson, David B, "Routing in Ad Hoc Networks of Mobile Hosts," *Proceedings of the IEEE Workshop on Mobile Ad Hoc Computing Systems and Applications,* December 1994.

Levis, Alexis, Chief Scientist of the Air Force, Private interview with the author, 16 March, 2004.

Morning, Frank. Jr., "Smallsats Grow Up," *Aviation Week & Space Technology.* 8 December, 2003.

Navy Warfare Development Command, "FORCEnet Brief," January 2004.

Oakes, Chris. “Getting Ahead of the Elliptic Curve.” Wired News, Wired.com. January 13, 1998. Located at http://www.wired.com/news/technology/0,1282,9634,00.html. Last accessed September 2004

Pigeau, Ross and Carol McCann. “Re-conceptualizing Command and Control.” *Canadian Military Journal Vol 3, No. 1.* Spring 2002.

Sklar, Bernard (2001). *Digital Communications: Fundamentals and Applications (2nd Edition).* Upper Saddle River, New Jersey, Prentice Hall PTR.

Smith, Edward. A. (2002). *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War.* Washington, Department of Defense Command and Control Research Program.

United States Geological Survey, “Metadata in Plain Language.” Document can be found at http://geology.usgs.gov/tools/metadata last accessed September 2004.

University of California San Diego, California Institute for Telecommunications and Information Technology, Demonstration and presentation. 19 February, 2004.

Walker, Rob ”Evolution to Net-Centric Operations,” Defense Information Systems Agency, April 2004.

Walker, Rob, “GIG Enterprise Services Piloting,” Defense Information Services Agency, April 20, 2004.

THIS PAGE INTENTIONALLY LEFT BLANK

BILBLIOGRAPHY

ABIS Task Force (1996). *Advanced Battlespace Information System (ABIS) Task Force Report – Major Results: Future Operational C2 System Capabilities and Enabling Technologies.*

Blackledge, Peter. (2004). "FORCEnet: Implementing Transformation, Joint Interoperability, and Network Centric warfare."

Department of Defense (2000). *Joint Vision 2020.* Washington, U.S. Government Printing Office.

Gladwell, Malcom (2000). *The Tipping Point: How little Things Can Make a Big Difference*. New York, Little, Brown and Company.

Moffat, James. (2003). *Complexity Theory and Network Centric Warfare.* Washington, Department of Defense Command and Control Research Program.

Myers, Richard B. (2004). *National Military Stratgey of the United States of America.* Washington, Department of Defense.

Watts, Duncan J. (1999). *Small Worlds: The Dynamics of Networks between Order and Randomness.* Princeton, New Jersey, Princeton University Press.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Marine Corps Representative
   Naval Postgraduate School
   Monterey, California

4. Director, Training and Education, MCCDC, Code C46
   Quantico, Virginia

5. Director, Marine Corps Research Center, MCCDC, Code C40RC
   Quantico, Virginia

6. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
   Camp Pendleton, California

7. Head, Information Operations and Space Integration Branch, PLI/PP&O/HQMC
   Camp Pendleton, California

8. Dan C. Boger
   Naval Postgraduate School
   Monterey, California

9. William Kemple
   Naval Postgraduate School
   Monterey, California