Fleet Cyber Command/TENTH Fleet: Enabling Cyber Unity of Effort

Lcdr Joseph E. Sisson, USN

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

The rapid advance of technology and the world's dependence on the internet and telecommunications for personal, business, and government activities has provided a new domain--cyber--to be exploited and attacked by U.S. adversaries. In order to counter this growing threat a transformation within the U.S. Department of Defense has begun with the establishment of U.S. Cyber Command (CYBERCOM) and the Navy cyber component, Fleet Cyber Command/TENTH Fleet. Fleet Cyber Command/TENTH Fleet is an organization that was established to harness the myriad missions currently in Navy doctrine to produce an economy of force and unity of effort across the four fields of information, intelligence, communications and command and control (C^2) to create a force capable of conducting and supporting operations in cyberspace. Fleet Cyber Command/TENTH Fleet's command organization and relationships will enable it to achieve unity of effort by fusing Navy's cyber, information operations, cryptologic and space capabilities under the command and control of a single commander.
Fleet Cyber Command/TENTH Fleet: Enabling Cyber Unity of Effort

by

Joseph E. Sisson

Lieutenant Commander / U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____________________

03 May 2010
Contents

Introduction 1

What Does Cyber Mean? 3

Vulnerability and Threat 6

Command Organization 8

Unity of Effort Through Unity of Command 15

A Counter Argument: Violating the Simplicity Tenant 17

Recommendations 19

Bibliography 20
## List of Illustrations

<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Warfare Domain's Relationship with Cyberspace</td>
<td>5</td>
</tr>
<tr>
<td>2.</td>
<td>World Internet Usage Statistics</td>
<td>7</td>
</tr>
<tr>
<td>4.</td>
<td>USCYBERCOM Organization</td>
<td>9</td>
</tr>
<tr>
<td>5.</td>
<td>Fleet Cyber Command/TENTH Fleet Organization</td>
<td>10</td>
</tr>
<tr>
<td>6.</td>
<td>Original TENTH Fleet Establishment Message</td>
<td>11</td>
</tr>
<tr>
<td>7.</td>
<td>TENTH Fleet Standing Task Organization</td>
<td>18</td>
</tr>
</tbody>
</table>
Abstract

The rapid advance of technology and the world's dependence on the internet and telecommunications for personal, business, and government activities has provided a new domain--cyber--to be exploited and attacked by U.S. adversaries. In order to counter this growing threat a transformation within the U.S. Department of Defense has begun with the establishment of U.S. Cyber Command (CYBERCOM) and the Navy cyber component, Fleet Cyber Command/TENTH Fleet. Fleet Cyber Command/TENTH Fleet is an organization that was established to harness the myriad missions currently in Navy doctrine to produce an economy of force and unity of effort across the four fields of information, intelligence, communications and command and control (C^2) to create a force capable of conducting and supporting operations in cyberspace. Fleet Cyber Command/TENTH Fleet's command organization and relationships will enable it to achieve unity of effort by fusing Navy's cyber, information operations, cryptologic and space capabilities under the command and control of a single commander.
The Challenge: Achieving Unity of Effort
"... separate ground, sea and air warfare is gone forever. If ever again we should be involved in war, we will fight it in all elements, with all services, as one single concentrated effort. Peacetime preparatory and organizational activity must conform to this fact. Strategic and tactical planning must be completely unified, combat forces organized into unified commands, each equipped with the most efficient weapons systems that science can develop, singly led and prepared to fight as one, regardless of service."¹

President Dwight D. Eisenhower

Introduction

The rapid advance of technology and the world's dependence on the internet and telecommunications for personal, business, and government activities has provided a new domain--cyber--to be exploited and attacked by U.S. adversaries.

President Obama addressed the importance of protecting the nation's cyber domain when he stated, "our technological advantage is a key to America's military dominance. But our defense and military networks are under constant attack. Indeed, in today's world, acts of terror could come not only from a few extremists in suicide vests but from a few key strokes on the computer -- a weapon of mass disruption."² In order to counter this growing threat a transformation within the U.S. Department of Defense has begun with the establishment of U.S. Cyber Command (CYBERCOM) and the Navy cyber component, Fleet Cyber Command/TENTH Fleet.³ Fleet Cyber Command/TENTH Fleet's command organization and relationships will enable it to achieve unity of effort by fusing Navy's cyber, information operations, cryptologic and space capabilities under the command and control of a single commander. The organizational relationships and the process of

synchronizing and sequencing actions, whether defensive or offensive in nature, amongst the many entities conducting operations across the cyber domain are instrumental in determining whether the United States will have an effective cyber capability.\textsuperscript{4} A cohesive, agile and resilient command organization is essential to enabling joint cyber operations in the 21\textsuperscript{st} Century. In order to create and maintain an effective joint cyberspace capability at the operational level unity of effort must be achieved between the organizations tasked with cyberspace missions.

This paper will focus on an analysis of the command organization of Fleet Cyber Command/TENTH Fleet to support the thesis that the establishment of this new organization empowers, not impedes, the joint force's cyber unity of effort. First, in order to frame the discussion, this paper will describe what constitutes cyberspace and how this warfare domain differs from the traditional land, air and sea domains in terms of Operational Factors time, space and force. Also, it will provide context to the cyber threat posed to the United States. Second, this paper will analyze the current Fleet Cyber Command/TENTH Fleet command organization, missions and relationships and discuss how unity of effort can be achieved through unity of command and organizational command and control (C\textsuperscript{2}). Third, this paper will consider a counter-argument to the thesis that Fleet Cyber Command/TENTH fleet will fail to achieve unity of effort by violating a basic Operational Command Organization tenant--simplicity.\textsuperscript{5} Finally, based on the analysis of the command organization and relationships this paper will present three recommendations to aid the achievement and maintenance of unity of effort.

\textsuperscript{5} Ibid, VIII-13.
Framing the Discussion: What does "Cyberspace" Mean?

Cyberspace and information environment are terms sometimes used interchangeably, although they have distinctly separate meanings. Cyberspace is a global domain within the information environment consisting of networks of information technology (IT) infrastructures, including the Internet, telecommunications networks, and computer systems. Effectively, this translates to the hardware and networks that store and transport information. The information environment is the aggregate of all people, organizations, and systems that collect, process, disseminate, or act on information. A clear understanding of what cyberspace is will help the reader visualize a "digital sea" that exists within the warfare domain with physical boundaries of IT hardware.

Today's domain of operations in cyberspace evolved from Command and Control Warfare (C2W) as defined by the Chairman of the Joint Chiefs (CJCS) Memorandum of Policy (MOP) 30 in 1993:

The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities, while protecting friendly capabilities against such actions. Command and Control Warfare applies across the operational continuum and all levels of conflict.

As technology evolved, and the proliferation of networked communications exploded around the world, cyberspace became a recognized warfare domain along with land,

---

6 Chairman, U.S. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Publication (JP) 1-02 (Washington, DC: CJCS, as amended through 31 October 2009), 139.
7 Ibid, 260.
air, maritime and space as outlined in the National Military Strategy for Cyberspace Operations. This warfare domain designation was a result of operational forces having the ability to conduct the six Operational Functions of warfare entirely within cyberspace: Maneuver being accomplished by freedom of movement and action across the information environment; Fires conducted by computer network attack (CNA) and electronic warfare (EW); Protection of friendly networks and information through computer network defense (CND) actions; Sustainment of networks and communications capabilities by network operations (NETOPS); Intelligence derived from data and information gained via computer network exploitation (CNE) and electronic warfare support (ES); and C² by operational commanders exercising authority and direction over assigned forces regardless of factor space. Operations in the cyberspace domain expand the traditional boundaries of warfare from land, air, maritime and space. Consideration toward unity of effort must be given since cyberspace transcends the physical boundaries of the geographical combatant commanders and theater of operations.

The Operational Factor of space for land, maritime and sea warfare is more easily defined that that of cyberspace. Identifying the attributes of factor space in terms of topography, people, distances, positions and shapes is more readily applicable to warfare on land, at sea and in the air. Cyberspace is not limited by physical boundaries and transcends geographical and functional boundaries allowing a commander to potentially control forces from thousands of miles away. However,

---

because cyberspace also consists of equipment that is installed at some physical location, a relationship between physical space and cyberspace does exist (Fig. 1).\textsuperscript{10}

\begin{center}
\begin{figure}
\includegraphics[width=\textwidth]{fig1}
\caption{War Fighting Domain's Relationship with Cyberspace}
\end{figure}
\end{center}

Time is the Operational Factor most affected by the advent of cyberspace operations. Considered the most precious and critical factor, time cannot be recovered once lost whereas space lost can be regained.\textsuperscript{11} Enabling near-simultaneous communications with assigned forces allows a commander to decrease the amount of time required to communicate operational plans, prepare, mobilize and deploy forces. Cyberspace allows a commander to shorten the decision-making cycle while affording greater flexibility during the course of operational warfare.

Of the three Operational Factors, force provides U.S. adversaries the greatest opportunity to gain an advantage and cause harm to U.S. interests. Over a decade ago Director of Central Intelligence, George Tenant, testified to Congress that "countries

\begin{flushright}
\textsuperscript{11} Ibid, III-19.
\end{flushright}
recognize that cyber attacks - possibly launched from outside the US - against civilian computer systems in the US - represent the kind of asymmetric option they will need to "level the playing field" during an armed crisis against the United States."12 His statement demonstrates that adversaries have the means to conduct cyber attacks against the U.S. across the diplomatic, information, military and economic (DIME) spectrum in order to neutralize any advantage the U.S. may have in combat power.

**Vulnerability and Threat**

Today the DoD operates more than one thousand five-hundred different computer networks across four thousand military installations around the world.13 According to the 2010 Quadrennial Defense Review (QDR) report, on any given day, there are as many as seven million DoD computers and telecommunications tools in use in eighty-eight countries providing a staggering number of possible vulnerabilities to our cyberspace and information domain. For context of the global scale of internet usage and growth see figures 2 and 3. Figure 2 provides data on the worldwide usage and growth of the internet while figure 3 depicts a snapshot in time of media usage on a given day (21 April 2010). The exponential growth in global internet penetration and the sheer volume of internet users requires an economy of force in cyber operations that will be enabled by unity of effort between Fleet Cyber Command/TENTH Fleet and CYBERCOM. America's cyberspace and information environment are critical vulnerabilities of the joint force and must be protected.

---

The importance of protecting and defending our country's cyberspace domain is highlighted throughout nearly every national strategy and policy document published over the past decade. The February 2010 Quadrennial Defense Review (QDR), a study conducted every four years by the Department of Defense to confront current and future challenges and serve as a means to develop new policies, capabilities and initiatives, identifies cyberspace as a national security vulnerability. Additionally, the QDR identifies the ability to "operate effectively in cyberspace" as one of the six key missions of the DoD over the next four
years. The scale of the Department of Defense's reliance on networked communications makes freedom of operations in cyberspace a de facto critical requirement for joint force operations in the 21st Century.

**Command Organization**

"It's also very important that TENTH Fleet settle into the relationship that exists between it and the joint headquarters above it and the work they do for STRATCOM (U.S. Strategic Command). Getting those relationships established is key." Admiral Gary Roughead

Chief of Naval Operations

The overarching Department of Defense organizational structure for commanding and controlling U. S. joint forces is defined by the Unified Command Plan (UCP). The UCP establishes unified and specified commands, assigns missions and functions to those commands, provides for assignment of forces, defines geographic areas of responsibility (AORs), delineates the chain-of-command and establishes command relationships.

In June 2009, Secretary of Defense Robert M. Gates established CYBERCOM as a subordinate unified command of U.S. Strategic Command. CYBERCOM's mission is to plan, synchronize and conduct defense of the Department of Defense information networks as well conduct full spectrum cyberspace operations when directed. In addition to the establishment of CYBERCOM, Secretary Gates ordered the military departments to "identify and provide appropriate component support to USCYBERCOM". As a result, the Chief of Naval Operations (CNO) established Fleet Cyber Command and re-commissioned TENTH

---

14 Ibid, 2.
17 William M. Gates, Secretary of Defense, Department of Defense, to Secretaries of the Military Departments, memorandum, 23 June 2009.
19 Ibid
Fleet as the Navy’s component to CYBERCOM. The Department of Defense cyber organization is depicted by a standard block organization chart as shown below (Fig. 4).

Fig. 4. USCYBERCOM Organization (http://www.govexec.com/nextgov/)

This graphic illustrates the many organizations tasked with cyber missions with multiple lines of administrative and operational control as well as the relationships of supported and supporting commanders. This command organization for the Department of Defense cyber forces provides the structure for a chain of command and relationships identifying command and support functions. Additionally, these relationships help identify the "...type and degree
of authority one commander has over another and the type and degree of support that one commander provides to another.”

Fleet Cyber Command/TENTH Fleet is an organization that was established to harness the myriad missions currently in Navy doctrine to produce an economy of force and unity of effort across the four fields of information, intelligence, communications and C² (Fig. 5). The goal is to create a force capable of conducting and supporting operations in the cyberspace warfare domain. The Navy's cyber force of Fleet Cyber Command/TENTH Fleet consists of fourteen thousand Sailors and civilians at more than twenty commands dispersed worldwide conducting missions in computer network operations, signals intelligence, naval communications and information operations.²¹,²²

![Fig. 5. Fleet Cyber Command/TENTH Fleet Organization](image)

The establishment of Fleet Cyber Command and the concurrent re-commissioning of the TENTH Fleet as the Navy’s component to CYBERCOM has been referred to as the

---


²¹ Commander, Fleet Cyber Command to Fleet Cyber Command forces, message 291700Z JAN 09, 29 January 2009.

reemergence of a “fleet-in-being” concept implemented with the original TENTH Fleet during World War II.23 During World War II, Admiral Ernest J. King, Chief of Naval Operations, established the original TENTH Fleet to “exercise unity of control over U.S. anti-submarine operations in that part of the Atlantic under United States strategic control (Fig. 6).”24

Fig. 6. Original TENTH Fleet Establishment Message (FLTCYBERCOM/TENTH Fleet Powerpoint)

This fleet command’s structure and authority enabled it to forge a close relationship between intelligence, research, development and operations in support of the anti-submarine warfare effort in the Atlantic Ocean. Ladislas Farago, in his 1962 book The Tenth Fleet, described

---

24 Naval Message, COMINCH 19 MAY 1943
the idea behind this organization as being "...to harness in a single, small and flexible, essentially intellectual unit of the best of brainpower to aid the combat elements of conventional seapower in their physical struggle with the U-boats--to put teeth into the anti-U-boat campaign by fusing brain and brawn."25 Today's Fleet Cyber Command/TENTH Fleet is poised to impact warfare in the cyber domain much as the 20th Century TENTH Fleet successfully enabled U.S. anti-submarine operations in the Atlantic. TENTH Fleet will provide worldwide operational support to commanders for cyberspace operations supporting the forces at sea and ashore in the joint and combined operational environments of the future. 26

Fleet Cyber Command/TENTH Fleet has been charged with multiple complex and varied missions related to cyberspace operations. The Chairman of the Joint Chiefs has referred to cyberspace operations as "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operations and activities to operate and defend the Global Information Grid." 27, 28 These missions range from the supporting roles that enable operations in the cyber domain to missions that focus on the protection and integrity of our own information and the networks on which it resides and is transferred. The supporting function of intelligence is necessary to enable effective cyberspace operations.

26 Chief of Naval Operations, to Commander, U.S. Fleet Forces Command and Director of Naval Intelligence, memorandum, 23 July 2009.
28 Department of Defense, Management of the Department of Defense Information Enterprise, Department of Defense Directive (DODD) 8000.01 (Washington, DC: DoD, 10 February 2009), 10. The Global Information Grid (GIG) is defined as the globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.
Specifically, signals intelligence (SIGINT) support to cyber operations is achieved through the relationship Fleet Cyber Command has with National Security Agency/Central Security Service (NSA/CSS), as the Navy's Service Cryptologic Component (SCC). Fleet Cyber Command/TENTH Fleet has invested manpower billets in the form of Cryptologic Technician (CT) sailors and Information Warfare Officers into NSA/CSS organizations around the world. The synergy of an integrated national-operational-tactical force focused on delivering usable intelligence to the warfighter and decision maker has historically been possible because of unity of effort across many organizations.

The original TENTH Fleet's development of new operating concepts for anti-submarine warfare achieved the effect of marginalizing the German threat to allied convoys. This significant achievement was enabled by the unity of effort that allowed the Operational Functions of intelligence, C², protection, movement/maneuver, fires and logistics operations to become welded and seamless under one commander. The Function of intelligence proved especially integral to defeating the German U-boat threat and provides an example, through lessons learned, for operations in cyberspace today. Since intelligence and operations were seamless, immediate access to all sources of information affecting the prosecution of German submarines in the Atlantic was available. Human intelligence (HUMINT) cultivated from interrogations of captured U-boat crews; signals intelligence based on radio intercepts of submarine communications; and U-boat locations derived from high frequency direction finding (HFDF) collectively aided TENTH Fleet in developing a deep understanding of German U-boat doctrine. This deep understanding was used to develop anti-submarine concepts of operation and assisted in localizing the enemy threat for prosecution by U. S. Navy surface ships. This historical example of an operational commander's staff employing
highly trained and educated personnel to process and analyze information gathered by many
varied methods and successfully generating operational effects is an example of how today's
TENTH Fleet can be successful.

Fleet Cyber Command and TENTH Fleet, while organizationally integrated, have
separate missions of providing support and effects at different levels of war. Fleet Cyber
Command is the Navy's component supporting CYBERCOM and is responsible for assisting
with the planning, execution and integration of joint cyber warfare capabilities into the
operational plans of the combatant commanders while directing Navy cyber operations at the
operational-strategic level of war. Additionally, Fleet Cyber Command, as the Navy's
Service Cryptologic Component, continues the legacy of providing signals intelligence
support to the NSA/CSS.\textsuperscript{29} In the TENTH Fleet capacity, the Commander is tasked with
providing operational support to Navy commanders worldwide at the operational-tactical
level of war in the areas of cyber, information and computer network operations, electronic
warfare and space.\textsuperscript{30} Together, Fleet Cyber Command/TENTH Fleet has been designated the
Navy's cyber component and is under operational control (OPCON) to CYBERCOM while
the Chief of Naval Operations maintains administrative control (ADCON) of the forces.

To align Navy cyber planning and capabilities with supported combatant commanders
and fleet commanders, TENTH Fleet will establish a Maritime Operations Center (MOC) at
its headquarters located at Ft. George G. Meade, MD. The purpose of standing up a TENTH
Fleet MOC is to support Fleet Cyber Command, combatant commanders and Fleet
commanders while integrating with U.S. Strategic Command/CYBERCOM Operations

\textsuperscript{29} Commander, Fleet Cyber Command to Fleet Cyber Command forces, message 291700Z JAN 10, 29 January
2010.
\textsuperscript{30} Ibid.
Centers. The MOC construct will streamline the operational decision cycle and provide a structure for quickly and effectively establishing support to an operational level commander. Imbedding TENTH Fleet liaison officers (LNOs) into each MOC in order to ensure mutual understanding and unity of effort will aid in reducing friction and fog between the multiple commands conducting cyber operations. The use of LNOs will be just one more action to ensure the "seams" between intelligence, information operations and space are welded to support operational planning of Navy support to the combatant commanders.

Unity of Effort Through Unity of Command

Dr. Milan Vego refers to the concept of jointness as "...contributing to unity of effort by focusing all the energy of individual services and the armed forces as a whole across the full range of military operations, at all levels of war and in every environment—peace, crisis, and war—toward enhancing the effectiveness of military operations." Unity of effort is ensured by unity of command across the DoD organizations tasked with cyber missions. Keys to achieving this unity is through clearly articulated intentions and objectives by the Commander of CYBERCOM to supporting commanders; Fleet Cyber Command providing advanced cyber-related education to its personnel; the development and assured understanding of cyber doctrine; and fostering an environment of trust at all levels of command.

Developing a process, not just a system, to command and control the cyber forces is also essential to assuring unity of effort through unity of command. The process of

---

31 Commander, Fleet Cyber Command to Fleet Cyber Command forces, message 290007Z DEC 09, 29 December 2009.
command and control (C$^2$) refers to the individual, but interrelated, functions of "command" and "control". Command is the authority that a commander exercises over subordinates while using available resources in accomplishing assigned missions$^{34}$ while control is how the commander implements his directives and establishes limits, focuses efforts, and provides a command structure.$^{35}$ Key to enabling successful command and control are the tenants of centralized direction and decentralized execution. Centralized direction ensures unity of effort through unity of command, aids decision making, empowers economy of force, eliminates uncertainty and maximizes control.$^{36}$ The assignment of one commander, "dual-hatted" as Fleet Cyber Command and TENTH Fleet, to oversee the operational-strategic and operational-tactical missions of Navy cyber forces ensures unity of effort through centralized direction. Equally as important to effective C$^2$ is the tenant of decentralized execution which allows for the delegation of authority to subordinate commanders.$^{37}$ In layman's terms, decentralized execution is the capacity for a subordinate who has been delegated authority to accomplish the commander's objectives with freedom of action. This tenant commends a trust the commander has bestowed in a subordinate to act with good judgment and skill. The following paragraph provides a historical example of how unity of effort was achieved by applying the tenants of command and control during the Battle of Trafalgar.

The British fleet in the Battle at Trafalgar is an example of centralized command and decentralized execution. Admiral Lord Nelson's victory over the combined fleets of the Spanish and French navies was made possible by his clear command intent, competence


among his fleet's captains, a deep understanding of the battlespace, and trust among the leaders (captains) in his fleet. The tactics which the British would employ against the superior enemy force were repeatedly discussed and practiced during the months spent searching for the enemy fleet. So, by the time the battle arrived each ship knew precisely their place in formation and the tactics to be executed. Equally important was Lord Nelson's reliance and trust in his captains' judgment and initiative to react in accordance with his guidance even during battle's unpredictable circumstances.  

Just as was the case with Lord Nelson's Fleet at the Battle of Trafalgar, Fleet Cyber Command/TENTH Fleet can successfully accomplish each of its diverse and complex missions so long as the commander clearly states his intent; educates his personnel; ensures understanding of a common operational concept and doctrine; and engenders trust at all levels of the organization.

A Counter-Argument: Violating the Simplicity Tenant

Although unity of effort is certainly obtainable through logical command organization and good leadership there does exist the possibility that unity of effort may fall short and become an impediment to effective joint cyber operations. A counter-argument to this paper's thesis is that Fleet Cyber Command/TENTH fleet will fail to achieve unity of effort by violating a basic Operational Command Organization tenant--Simplicity.

The commander of Fleet Cyber Command/TENTH Fleet is tasked with overseeing the Navy's forces and capabilities conducting cyber, information, space and network operations in support of CYBERCOM, the combatant commanders and Fleet commanders.

---

Additionally, the commander of Fleet Cyber Command is responsible for providing signals intelligence support to the NSA/CSS in his role as the SCC commander.

According to Dr. Vego, a sound command organization should be simple above all else. Considering the sheer size of Fleet Cyber Command/TENTH Fleet: 14,000 Sailors and civilians; the myriad and varied missions assigned: cyber, information operations, signals intelligence, computer network operations, electronic warfare and space operations; and the scope of supported commander relationships: CYBERCOM, combatant commanders, Fleet commanders, and tactical units, it appears Fleet Cyber Command/TENTH Fleet is the antithesis of a "simple" command organization and, for this reason, could fail to achieve unity of effort.

Mitigating these complex factors is a clearly delineated chain-of-command with one commander providing unambiguous direction and intent across a well-defined Standing Task Organization (Fig. 7); the establishment of a TENTH Fleet MOC providing support the combatant commanders and Fleet commanders; and the integration of LNOs at each MOC.

Fig. 7. TENTH Fleet Standing Task Organization
So, while the command organization is large and not simple, Fleet Cyber Command/TENTH Fleet will be successful in achieving unity of effort by fusing Navy's cyber, information operations, cryptologic and space capabilities under the command and control of a single commander.

**Recommendations**

The Commander of Fleet Cyber Command/TENTH Fleet will best foster unity of effort through following recommendations:

- Invest in the establishment of an advance education program that develops intellectual capital in the cyber force. Partner with civilian academia to expand the opportunities to attain Master- and Doctoral-level degrees in the areas of computer science, electrical and computer engineering, mathematics, and focused regional studies in order to retain a highly skilled workforce.

- Integrate TENTH Fleet liaison officers (LNOs) at each MOC to ensure mutual understanding and unity of effort across supported/supporting commanders.

- Develop an overarching Navy cyber doctrine that nests with Joint cyber doctrine and ensure the Navy's cyber force understands the doctrine conceptually and in practice.


Chief of Naval Operations. To Director of Naval Intelligence. Memorandum, 26 June 2009.

Chief of Naval Operations. To Commander, U.S. Fleet Forces Command and Director of Naval Intelligence. Memorandum, 23 July 2009.


Commander, Fleet Cyber Command. To Fleet Cyber Command, Message. 290007Z DEC 09. 29 December 2009.


Roughead, ADM Gary, Chief of Naval Operations. To Commander, Fleet Forces Command and Director of Naval Intelligence. Memorandum. 23 July 09.


Starling, VADM Denby. “CYBERFOR/NETWARCOM Staff Alignment.” Powerpoint. 05 February 2010.


