Strategy Research Project

CAN THE NAVY'S TENTH FLEET EFFECTIVELY COMBAT THE CYBER THREAT?

BY

COMMANDER ALBERT ANGEL
United States Navy

USAWC CLASS OF 2010

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
25-03-2010	Strategy Research Project	

4. TITLE AND SUBTITLE

Can the Navy's Tenth Fleet Effectively Combat the Cyber Threat?

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Commander Albert Angel

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Lieutenant Colonel John A. Mowchan
Center for Strategic Leadership

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

During World War II, the U.S. faced a burgeoning technological threat to its security with the advent of Germany's unrestricted submarine warfare. The U.S. Navy faced this danger head on and stood up Tenth Fleet to protect allied shipping and convoys through the expanded use of intelligence and information to significantly diminish the U-boat threat. In 2009, the U.S. Navy reconstituted its Tenth Fleet to again confront a dangerous and growing threat, this time in cyberspace. Although cyberspace has greatly enhanced the way people communicate, conduct business and relate to each other, it has also allowed for some severe unintended consequences, namely the ability for state and non-state actors to use this domain to cause us harm. This modern cyber threat is growing rapidly and poses a serious risk to our nation's economic and national security interests. This paper explores the historical roots of Tenth Fleet and the innovation and lessons learned during WWII to better enable the reconstituted Tenth Fleet to protect, deter and defend against the growing cyber threat.

15. SUBJECT TERMS

Information Dominance, Network, Computer Attack, Deterrence

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	42	

USAWC STRATEGY RESEARCH PROJECT

CAN THE NAVY'S TENTH FLEET EFFECTIVELY COMBAT THE CYBER THREAT?

by

Commander Albert Angel
United States Navy

Lieutenant Colonel John A. Mowchan
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Commander Albert Angel

TITLE: Can the Navy's Tenth Fleet Effectively Combat the Cyber Threat?

FORMAT: Strategy Research Project

DATE: 25 March 2010 WORD COUNT: 7,738 PAGES: 42

KEY TERMS: Information Dominance, Network, Computer Attack, Deterrence

CLASSIFICATION: Unclassified

During World War II, the U.S. faced a burgeoning technological threat to its security with the advent of Germany's unrestricted submarine warfare. The U.S. Navy faced this danger head on and stood up Tenth Fleet to protect allied shipping and convoys through the expanded use of intelligence and information to significantly diminish the U-boat threat. In 2009, the U.S. Navy reconstituted its Tenth Fleet to again confront a dangerous and growing threat, this time in cyberspace. Although cyberspace has greatly enhanced the way people communicate, conduct business and relate to each other, it has also allowed for some severe unintended consequences, namely the ability for state and non-state actors to use this domain to cause us harm. This modern cyber threat is growing rapidly and poses a serious risk to our nation's economic and national security interests. This paper explores the historical roots of Tenth Fleet and the innovation and lessons learned during WWII to better enable the reconstituted Tenth Fleet to protect, deter and defend against the growing cyber threat.

CAN THE NAVY'S TENTH FLEET EFFECTIVELY COMBAT THE CYBER THREAT?

> When war has been accepted as necessary, success means nothing short of victory; and victory must be sought by offensive measures…
>
> —Alfred T. Mahan[1]

On 23 July 2009, Admiral Gary Roughead, U.S. Navy Chief of Naval Operations (CNO), directed the Navy to stand up its newest operational command, Tenth Fleet, under the auspices of U.S. Fleet Cyber Command. Per guidance issued by the Secretary of Defense, the Navy was tasked to identify and provide component support to the newly established U.S. Cyber Command no later than 1 October 2009.[2] As such, the CNO directed that the Director of Naval Intelligence lead an implementation team and develop a plan for Fleet Cyber Command to be stood up as the Navy's Component Commander to U.S. Cyber Command at Ft Meade, MD.[3] Additionally, Tenth Fleet was to be reconstituted and serve as the lead for Navy operations in cyberspace.[4] It is not unusual for a military service to stand up a new organization during a time of transformation or to counter a growing threat. The U.S. Navy is no exception and this marks the second time that the Navy has stood up the Tenth Fleet to address a burgeoning threat to national security.

Origins of Tenth Fleet

The first incidence involving Tenth Fleet took place in the Spring of 1943, when allied shipping was facing a seemingly insurmountable threat from German submarines, or U-boats, during World War II. Prior to this time, the anti-submarine effort was decentralized and parceled out among the sea frontiers,[5] naval districts, fleet commanders, as well as divided among the United States, the United Kingdom, Canada, and Brazil.[6] The threat posed by German submarines was so significant that

during the Casablanca Conference, 19 January 1943, the Combined Chiefs of Staff (CCS),[7] President Roosevelt and Prime Minister Churchill each agreed that the defeat of the U-boat was of great importance and needed to be addressed.[8] From January to March of 1943, losses of merchant shipping destroyed by U-boats rose steadily to a high of 108 allied ships, which corresponded to 627,000 tons.[9] On 30 April 1943, the CCS recommended that each allied nation centralize its control of anti-submarine warfare and cooperate closely in the study and integration of the anti-submarine effort.[10] Thus, on 1 May 1943, Admiral Ernest King assumed control of the disparate U.S. anti-submarine effort during World War II and unified these units with the establishment of Tenth Fleet.[11]

After seventeen months since the commencement of hostilities marking the entry of the U.S. into World War II, the U.S. Navy formed an organization responsible for the formulation and execution of operational strategy for the anti-submarine campaign.[12] Tenth Fleet directed the efforts of the hunter-killer groups composed of escort carriers, destroyers and destroyer escorts assigned to the Atlantic Fleet.[13] Commander Tenth Fleet exercised direct control over all of the Atlantic Sea Frontiers, which were comprised of the Eastern, Caribbean and Gulf Sea Frontiers, and used the Sea Frontier Commanders as Task Force Commanders.[14] Although no ships were assigned to Tenth Fleet, it had the authority to direct all anti-submarine activity and to detach naval surface and air assets, as needed, from the various Atlantic Commands.[15] Moreover, Tenth Fleet had a broad mandate to execute its mission; search and destroy enemy submarines, protect allied shipping, support other anti-submarine forces, exercise control over convoys and routing, and correlate training and materiel development.[16] By

the summer of 1943, Tenth Fleet had developed into a truly unified organization that concentrated all anti-submarine efforts, to include intelligence, force allocation, control of convoys and the development of tactical doctrine to best confront the U-boat threat.[17]

Defeating the U-boat

There were a number of factors that contributed to the allies' victory over the U-boat. One of Tenth Fleet's key elements was a strong intelligence unit, OP-20G, under its Operations Division, that had its own Submarine Tracking Room with ready access to ULTRA (data decrypted from Enigma machines[18]) and HF/DF (High Frequency Direction Finding) fixes.[19] Another critical factor was the contribution of civilian scientists in the development of doctrine and improved weapons that would prove decisive in the spring and summer of 1943.[20] Scientists advocated and developed the use of Magnetic Anomaly Detection (MAD) devices, radio sonobuoys, retro-bombs and acoustic torpedoes to enable allied aircraft to better target and engage German U-boats.[21] Debate over campaign strategy and anti-submarine doctrine led offensive and defensive thinking in dealing with the U-boat threat; however, scientists would play a significant role in the development of both trains of thought.[22] For example, scientists would play a pivotal role in sponsoring and developing concepts for conducting offensive operations against the German U-boats; such as utilizing aircraft to attack known concentrations of U-boats before they got to the convoys.[23] By analyzing the data from a research perspective, scientists were able to develop new ways to better defend convoys and minimize their losses by providing more robust air and surface escorts.[24] In May 1943, communications intelligence derived from OP-20G, advances in radar, improved weather, and a host of new weapons, to include the Mark XXIV acoustic torpedo, enabled allied aircraft to track, target and engage U-boats, which up

to this point had enjoyed operational and tactical invisibility.[25] The allied effort against the U-boat would continue to gain momentum through the summer and fall of 1943 to a point in which the threat posed by the U-boat would soon be significantly diminished. On October 27, 1943, the losses incurred by the U-boat were such that Admiral King declared "submarines have not been driven from the seas, but they have changed status from a menace to a problem."[26] In the six months before Tenth Fleet was created, the U.S. Navy sank 36 U-boats; however, it sank 75 U-boats the following six months.[27] Thus, Tenth Fleet was able to accomplish its mission objectives in a short time and was able to minimize the threat of the U-boat and contribute significantly to the Allied victory in the Atlantic. Many of the lessons learned during the establishment of Tenth Fleet and execution of its mission, to include the importance of unity of effort, strong intelligence and tight cohesion between civilian scientists and military personnel, should be heeded as they served Tenth Fleet well in the past, and could do so again.

Cyberspace and Modern Threats

Sixty-five years after the end of World War II a new and arguably more potent threat, a cyber threat, has emerged that could potentially undermine peace and security throughout the world. This new threat is unlike any other in that it takes place in a man-made domain that does not inhibit, prevent or challenge access to the high seas, air space, or outer space, commonly referred to as the global commons.[28] The twenty-first century has born witness to unprecedented advancements in technology and no country more than the U.S. has immersed itself fully in the cyber age. Cyberspace has significantly altered the way people communicate, conduct business and relate to each other.[29] Our nation's critical infrastructure, composed of private and public institutions which control the electric power grid, telecommunications, Internet, financial system,

transportation management, air traffic control and other services, is largely managed and controlled through cyberspace via hundreds of thousands of interconnected computers, servers, routers, switches and fiber optic cables.[30] Thus, a healthy and functioning cyberspace is vital to our economy and national security.

Unlike the internationally recognized domains of air space, outer space or the high seas, cyberspace is not a traditional global common and there has been little effort to define or delineate the notion of cyber sovereignty.[31] While each government can try to manage its portion of cyberspace, they are all interconnected around the world and as highlighted in Figure 1, the cyber domain transcends physical boundaries.[32]

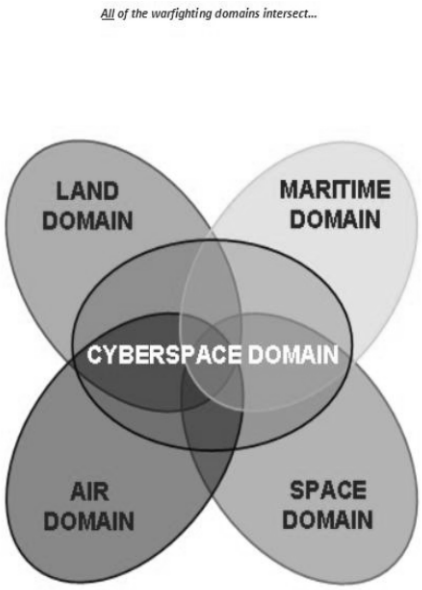

Figure 1. Cyberspace Domain contained within and transcends other Domains[33]

Data transmissions flow virtually unhindered in cyberspace without any regard for a nation's sovereignty, and anyone with access to cyberspace enjoys practically unfettered access to navigate and communicate in this domain.[34]

In the U.S. alone there were 5,488 breaches of government computer systems and 54,640 incidents of malicious cyber activity against the Department of Defense

(DoD) in 2008.[35] Although one can argue that cyberspace has greatly enhanced man's ability to communicate with one another, it has also allowed for some severe unintended consequences, namely the ability for state and non-state actors alike to use the domain to do significant harm with little fear of retribution. Cyber attack weapons are emerging as an ever-growing threat aimed at altering, disrupting, deceiving, degrading, and/or destroying computer systems or networks, which significantly increases the threat posed to our critical infrastructure and that of our allies.[36]

Baseline Definitions for Cyberspace Operations

While there has been some effort between U.S. government agencies, such as the Department of Homeland Security (DHS) and DoD, to outline baseline cyber definitions, these have not been widely accepted outside of the government although they have proven useful in developing doctrine to confront the cyber threat.[37] In many cases, events in cyberspace blend crime, espionage, and military action in ways that render them indistinguishable to those responsible for defending and responding to such incidents.[38] Ultimately, the decision as to whether an incident in cyberspace is an attack or constitutes an act of war rests with the nation's political leadership, as does the manner in which the nation responds.[39] For good reason, the cyberspace domain can be characterized by its vulnerability, uncertainty, complexity and ambiguity (VUCA).[40] Threats to cyberspace fall within six discrete categories: traditional, irregular, catastrophic, disruptive, natural and accidental.[41]

Currently, no international treaties have been widely endorsed to properly define cyber sovereignty or adequately deal with the problems posed by cyber crime, cyber attack, cyber espionage, cyber terrorism and cyber war. Arguably the most important effort at reaching some semblance of international cooperation on cyber crime took

place in Budapest, Hungary on 23 November 2001, when the Council of Europe convened a Convention on Cybercrime that was attended by representatives from 52 nations.[42] This marked the first multilateral instrument drafted to address the problems posed by the spread of criminal activity on computer networks.[43] The Council of Europe Convention on Cybercrime entered into force in July 2004 and remains the sole binding international treaty on the subject to date; however, with less than half of the attendees (22 as of 9 March 2009) ratifying the treaty, it makes it extremely difficult to lay down guidelines for governments wishing to develop effective legislation against cybercrime and boost international cooperation.[44] The lack of internationally agreed definitions exacerbates efforts to tackle these issues as there are numerous jurisdictions, laws, and caveats that often hinder efforts to deal with the problem in a multilateral arena. Often, nations are hindered in their ability to protect their networks against cyber attacks much less from trying to deter such attacks in the first place.

Cyber Threat to Critical U.S. Infrastructure

Shortly after taking office, President Obama identified the cyber threat as "one of the most serious economic and national security challenges we face as a nation."[45] The President ordered a thorough review of federal efforts to secure cyberspace and the development of a comprehensive whole of government approach to securing America's information and communications infrastructure.[46] The resulting Cyberspace Policy Review outlined several proposals, such as the need for an Executive Branch Cybersecurity Coordinator, commonly referred to as the White House Cyber Czar, to work closely with all key agencies involved in securing the digital infrastructure of the U.S.[47] The Review further posited that initiatives should build upon the Comprehensive National Cybersecurity Initiative (CNCI), which was first implemented by President

George W. Bush in January 2008.[48] One way the newly appointed White House Cyber Czar, Howard Schmidt, chose to enhance coordination and information sharing between agencies with the Federal government, to include DHS and DoD, was to publish an unclassified version of the CNCI.[49] The CNCI includes funding within federal law enforcement, intelligence, and defense communities to enhance the key areas of criminal investigation, intelligence, and information assurance.[50] To accomplish these functions, CNCI's mandate specifies:

> (a) establish a front line defense against today's immediate threats,
>
> (b) defend against the full spectrum of cyber threats, and
>
> (c) strengthen the future cybersecurity environment.[51]

Long before the CNCI was published, cybersecurity was on the national agenda and identified as a vital national security interest as these attacks have the potential to disable electrical power systems, corrupt financial data or hijack air traffic control system.[52] On 17 December 2003, Homeland Security Presidential Directive 7 (HSPD-7) established a national policy for federal departments and agencies to identify and prioritize critical infrastructure and to protect them from attacks.[53] As outlined in Table 1, the roles and responsibilities are wide ranging and require unity of effort. As such, HSPD-7 dictates that each sector-specific agency shall:

> (a) collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including key persons and entities in their infrastructure sector;
>
> (b) conduct or facilitate vulnerability assessments of the sector; and
>
> (c) encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.[54]

Federal Agency	Sector Responsibilities
Department of Agriculture	agriculture, food (meat, poultry, egg products)
Health and Human Services	public health, healthcare, and food (other than meat, poultry, egg products)
Environmental Protection Agency	drinking water and water treatment systems
Department of Energy	energy, including the production refining, storage, and distribution of oil and gas, and electric power except for commercial nuclear power facilities
Department of the Treasury	banking and finance
Department of the Interior	national monuments and icons
Department of Defense	defense industrial base

Table 1. Roles and Responsibilities of Sector-Specific Federal Agencies[55]

Attacks on U.S. infrastructure are significant and growing; this issue is pressing and requires immediate attention.[56] While the 2003 National Strategy to Secure Cyberspace (NSSC) outlines responsibilities for DHS to protect civilian and government networks and the 2006 National Military Strategy for Cyberspace Operations (NMS-CO) outlines responsibilities for DoD to protect the military's networks, there needs to be considerable effort and coordination between DHS and DoD to effectively counter the cyber threat to the U.S. More importantly, the CNCI offers a coherent strategy that augments those efforts specified by the NSSC and NMS-CO, thus ensuring a whole of government approach to countering the cyber threat.

Cyber Threat to U.S. Military

The U.S. military relies on cyberspace as a critical component of its military effectiveness to such an extent that the use of computer networks to gather, organize and move information may prove to be its Achilles heel in the information age.[57] This is

as evident today as it was in December 2006 when the NMS-CO correctly postulated that the U.S. military dependence on cyberspace would continue to increase.[58]

> DoD force transformation hinges largely on a move toward net-centric operations. Significant investments in force structure, infrastructure, and programs have oriented DoD components towards the use of cyberspace as an integral part of warfighting. Threat actors can take advantage of this dependence and adversely affect cyberspace operations.[59]

Currently, on any given day the DoD operates over 7,000,000,000 computers and telecommunication units via 15,000 computer networks across more than 4,000 military installations located in 88 countries utilizing thousands of warfighting and support applications.[60] Clearly, the magnitude and diversity of DoD configurations makes it difficult to maintain situational awareness and manage the computer network risks, much less the entire GIG.[61] Therefore, it is incumbent that the U.S. military take steps not only to perform its three main missions outlined in NMS-CO,[62] but also to ensure the ability to operate unhindered in cyberspace in order to conduct full spectrum operations across all the global commons.

Importance of Cyber Attribution

The Internet has provided a virtual safe haven for those who would threaten the U.S. military, to include non-state actors, terrorists, criminal groups and hackers.[63] By its very nature, cyberspace is a domain amenable to asymmetric warfare because it can be used anonymously, which makes it difficult to deter, let alone punish those who would exploit this domain for nefarious acts.[64] In order to defend, deter and punish we need to significantly improve our cyber forensics and attribution capability so that we can mitigate the advantages currently prevalent in cyberspace, namely stealth and anonymity. Improved attribution will also decrease the risk of “false flag” attacks, which allow perpetrators to mask their involvement or disguise it as an attack carried out by

another country.[65] However, before any organization can choose to expand their cyber operations from defensive to offensive (punitive/retaliatory), it must ensure it has the requisite forensics capacity to adequately attribute a cyber act to a particular perpetrator. Failure to properly attribute a cyber act to the responsible perpetrator prior to taking retaliatory action is sure to garner widespread condemnation and open the floodgates for would-be perpetrators to conduct cyber attacks of their own.

Cyber Defense and Deterrence

Much of our efforts on cyber security focus on defense, to include protecting computers, data and networks from unauthorized use or manipulation.[66] Cyber defense, protecting our computers and networks from attack, alone will do little to keep our nation safe from the growing attacks faced in this domain because every new firewall brings about a more robust virus or means for disabling or bypassing our security measures. While cyber defense is an important aspect for any cyber policy and one in which the U.S. should continue to invest, it is completely insufficient by itself in deterring the growing cyber threat. As noted earlier, the category of cyber threats highlighted in the NMS-CO, namely traditional, irregular, catastrophic, disruptive, natural and accidental, remains the same whether we are discussing civilian business networks, links to critical infrastructure, or DoD networks. HSPD-7 clearly delineates each federal organization that is responsible for defending their respective portion of the cyber domain; however, it is evident that cyber defense in not enough and the U.S. must develop a robust and comprehensive cyber deterrence and retribution policy against hostile actors. Such a deterrence policy needs to be widely disseminated and focus on all available military means to ensure there is no doubt as to what action the U.S. is prepared to take to defend its national security. While not all cyber attacks

would warrant retribution or be considered an act of hostility or war, we must recognize that our critical infrastructure is a vital national security interest. This means that all federal agencies assigned responsibilities for safeguarding elements of our critical infrastructure must work in a collaborative environment to ensure that all sectors are adequately defended from emerging cyber threats. A ladder of escalation will need to be reviewed to carefully consider those cyber acts that constitute a threat to our national security and those that may be deemed acts of sabotage, mischief, crime or espionage.

Although we are continually strengthening our cyber defensive and offensive capabilities and have unprecedented diplomatic and economic power to exert pressure on our foes, our true strength as a nation resides in our unmatched military strength. We need to make clear to the world that our critical infrastructure constitutes a vital national security interest and we are prepared to take appropriate measures to defend it. Moreover, there are clearly instances when an attack in the cyber domain would be comparable to an act of war and thus the U.S. must demonstrate that it will not hesitate to take quick and devastating action to deter and punish such attacks from taking place. While we will not hesitate to utilize the cyber domain to attack our enemies and deter aggression, we must ensure that all military means are available to adequately protect and defend our critical national interests from attack.

Tenth Fleet Re-emerges to Tackle Cyber Threat

In October 2007, the U.S. Navy CNO, Admiral Gary Roughead highlighted the seriousness of the growing cyber threat when he stated the following:

> The opening rounds of the next war will likely be in cyberspace – the Navy must be ready to prevent wars as well as win them; to do that, we must understand how we live, operate and win in cyberspace.[67]

Today's modern Navy requires "uninhibited access to assured communication capabilities in cyberspace."[68] More importantly, the Navy must be able to execute its full range of global missions when cyberspace is denied and must also be able to deny any enemy, be it a state or non-state actor, the ability to operate in cyberspace when it is appropriate or required.[69] The Navy has made some significant organizational decisions to realign its posture in the information age and be more effective in facing the cyber threat.[70]

On 1 October 2009, the Navy reorganized the Office of the Chief of Naval Operations (OPNAV) staff to achieve the requisite integration and innovation necessary for achieving warfighting dominance across the maritime, cyber and information domains.[71] The merging of the Intelligence directorate (N2) with the Communication Networks directorate (N6) into a single directorate, known as the Information Dominance Corps (N2/N6), will better enable the Navy to address the challenges in the Information Age.[72] The 44,000 active and Reserve Navy officers, enlisted and civilian professionals who comprise the Information Dominance Corps will be incorporated into each and every Navy organization associated with achieving warfighter dominance in the maritime, cyber and information domain, to include the newly reconstituted Fleet Cyber Command/Tenth Fleet. With this groundbreaking decision, the Navy is effectively elevating "Information" to a core warfighting capability on par with other naval combat competencies.[73] The first ever Deputy Chief of Naval Operations for N2/N6, Vice Admiral (VADM) David Dorsett, will be responsible for making investment decisions for information, cyber and space capabilities, and for also developing the Navy's information architectures.[74] According to VADM Dorsett, "the Information Dominance

Corps will create a cadre of information specialists, who come with individual community identities and unite to be managed as a corps, developed as a corps, and to fight as a corps."[75] The individual communities that will be merged into the Information Dominance Corps include information professional officers, information warfare officers, naval intelligence officers, meteorological and oceanography officers, space cadre officers, aerographer's mates, cryptologic technicians, intelligence specialist, information systems technicians and civilian personnel.[76] This is an extremely important and time-critical decision considering the guidance issued from the Chairman of the Joint Chiefs of Staff (CJCS) highlighting the fundamental need to protect the global commons of the sea, air, space and cyberspace.[77]

It came to no one's surprise on 23 June 2009 when Secretary of Defense Robert Gates ordered U.S. Strategic Command to establish a new cyber command by October 2009 and to have it fully functioning by October 2010.[78] U.S. Cyber Command would effectively unify the military's previously separate defensive and offensive cyberspace operations, the Joint Task Force-Global Network Operations and the Joint Functional Component Command-Network Warfare.[79] Shortly thereafter, each component of the military was tasked to provide component support to the newly established U.S. Cyber Command depicted below in Figure 2. The overarching mission will be on enhancing the organization of the cyber effort and adding much needed resources to accelerate development of DoD cyber capabilities and integrate them into its daily operations.[80] U.S. Cyber Command would focus solely on military computer networks and operations outlined in NMS-CO, leaving defense of civilian networks to DHS and its corresponding guidance in the NSSC.[81]

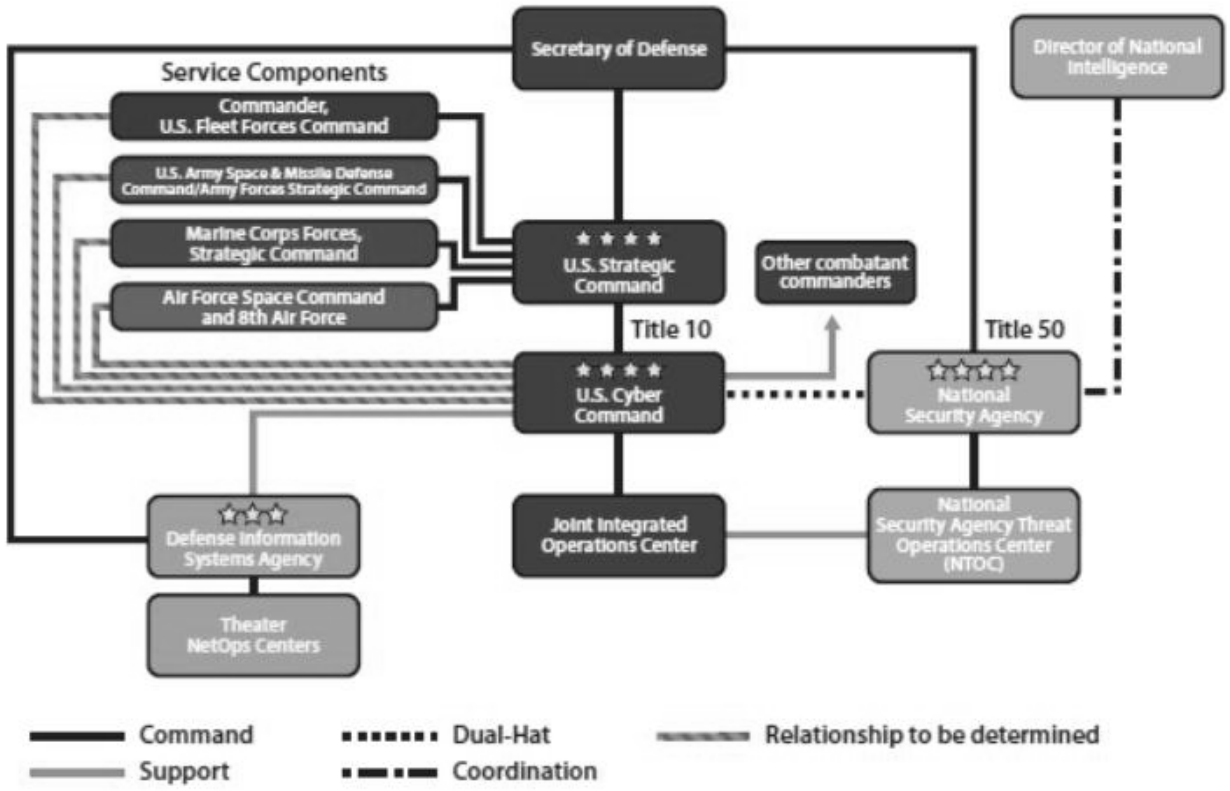

Figure 2. U.S. Cyber Command Organization[82]

On 23 July 2009, the CNO directed that Fleet Cyber Command/Tenth Fleet be established on 1 October 2009 to meet the tasking of the Defense Secretary.[83] Fleet Cyber Command/Tenth Fleet was established as a focused force organized to defend, exploit and achieve operational effects in and through cyberspace and to assure freedom of maneuver in cyberspace, which is vital to successful naval operations.[84] While Fleet Cyber Command will be under Administrative Control (ADCON) to the CNO, it will be under Operational Control (OPCON) to U.S. Cyber Command and will serve as its central operational authority for networks, intelligence, cryptology/signals intelligence (SIGINT), information operations (IO), cyber, electronic warfare, and space in support of naval forces ashore and at sea.[85] IO comprises multiple warfare disciplines, to include electronic warfare (EW), psychological operations (PSYOP), computer network

operations, military deception and operations security (OPSEC). Computer network operations itself reveal three further areas, which are computer network attack (CNA), computer network defense (CND), and computer network exploitation (CNE).[86] Success will only be possible by synchronizing Navy computer network operations capabilities such that CNA, CND and CNE are planned and executed as an integrated effort that complements Joint and National cyber efforts.[87] The specified mission of Fleet Cyber Command is as follows:

> to direct Navy cyberspace operations globally to deter and defeat aggression and to ensure freedom of action to achieve military objectives in and through cyberspace; to organize and direct Navy cryptologic operations worldwide and support information operations and space planning and operations, as directed; to direct, operate, maintain, secure and defend the Navy's portion of the Global Information Grid; to deliver integrated cyber, information operations cryptologic and space capabilities; and to deliver global Navy cyber network common cyber operational requirements.[88]

As directed by Fleet Cyber Command (depicted below in Figure 3), Commander Tenth Fleet will direct operations and provide operational support to Navy commanders worldwide in the area of cyber, information and computer network operations, electronic warfare, and space.[89] Tenth Fleet will be required to "direct and support operations to deter and defeat aggression, ensure freedom of action, and achieve military objectives in and through cyberspace across the full spectrum of military operations."[90] Fortunately for Tenth Fleet, it has a proud tradition of excellence passed down from its predecessor Command, which should serve it well as it fully engages this new cyber threat. During World War II, Tenth Fleet was an organization whose success "depended less on manned and massed fire power than on intelligence and information."[91] More important, as Tenth Fleet is tackling the cyber mission, "even more so than before, victory will be predicated on timely and accurate intelligence rather than fire power."[92] Thus, it would

serve Fleet Cyber Command/Tenth Fleet well to recognize the importance of unity of effort, strong intelligence and tight cohesion between civilian scientists and military personnel, the same tenets of success which assured Tenth Fleet of victory over the U-boat more than 60 years ago. The specified mission of Tenth Fleet is as follows:

> to serve as the Number Fleet for Fleet Cyber Command and exercise operational control of assigned Naval forces; to coordinate with other naval, coalition and Joint Task Forces to execute the full spectrum of cyber, electronic warfare, information operations and signal intelligence capabilities and missions across the cyber, electromagnetic and space domains.[93]

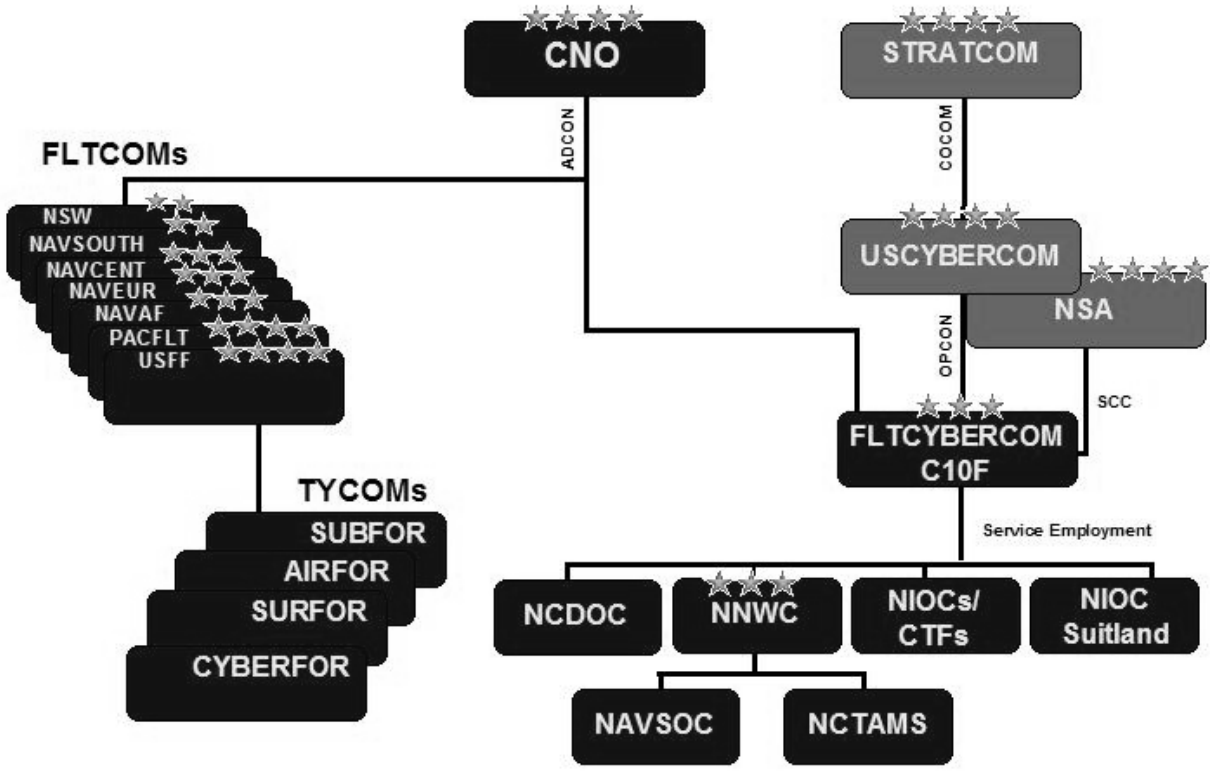

Figure 3. Navy Cyber Command and Control Relationships[94]

Tenth Fleet Forging Ahead

VADM Barry McCullough is dual-hatted as the Commander of both U.S. Fleet Cyber Command and the U.S. Tenth Fleet. On 29 January 2010, a ribbon-cutting ceremony was hosted by the CNO to commemorate Fleet Cyber Command/Tenth Fleet

achieving initial operational capability (IOC).[95] In order to ensure unity of effort in the cyber mission, Tenth Fleet will assume OPCON of the Navy's cyber, network operations, cryptologic and space forces; Naval Network Warfare Command (NAVNETWARCOM), Navy Cyber Forces (NAVCYBERFOR), the regional Navy Information Operations Commands (NIOCs), Navy Cyber Defense Operations Command (NCDOC) and Navy and Marine Corps Spectrum Center (NMCSC).[96] In short, NCDOC will focus on defensive cyber capabilities; NAVNETWARCOM will conduct network and space operations in support of naval forces; NAVCYBERFOR is the Type Commander (TYCOM) and will focus on maintaining and operating the computer networks, in addition to TYCOM responsibilities of manning, training and equipping cyber forces;[97] the 15 regional NIOCs will focus on forensics, attribution and providing cyber support to the fleets;[98] while NIOC Suitland (located at the Office of Naval Intelligence) will concentrate on target development.[99] Forensics and attribution are especially important in the cyber domain because failure to properly apply blame for a cyber attack by a state or non-state actor severely limits the ability of the strategic leadership to take appropriate action. Attribution isn't impossible to carry out in the cyber domain but just as in World War II when locating submarines was the most complex problem of the day, this new cyber problem can be tackled by leveraging the efforts of organic and outside organizations, particularly the expertise of civilian scientists.

VADM McCullough highlighted the importance of the intelligence effort to the cyber mission when he stated that Tenth Fleet "must be able to exercise command and control over our networks with dynamic, real time defense and information assurance

enabled by intelligence collection.[100] A strong intelligence capability will be fostered at Tenth Fleet and its regional NIOCs and must be leveraged with the intelligence entities at U.S. Cyber Command and its associated military components. Intelligence will be integral in profiling threats, enhancing defensive strategies, and recognizing and monitoring known/potential adversaries.[101] To maximize the role Tenth Fleet and her sister component cyber commands fulfill, it is critical that intelligence information be properly collected, analyzed, and disseminated in a timely manner with joint and national agencies responsible for safeguarding our nation's computer networks. While Tenth Fleet will eventually provide forces and capabilities to U.S. Cyber Command that could be used in an offensive manner, near term focus will be on network defense to ensure the Navy continues to enjoy unfettered access to cyberspace while carrying out its global missions.[102]

Tenth Fleet has established a Maritime Operations Center (MOC) to effectively plan, execute, control and monitor Tenth Fleet operations; support Fleet Cyber Command; align to U.S. Strategic Command's Operation Center, as directed; and will further align to the numbered fleets and other command and staff organizations, as required by mission tasking.[103] As Tenth Fleet approaches Full Operational Capability (FOC) on or about October 2010, it will need to develop a plan and associated requirements for participation in the U.S. Cyber Command Integration Team Concept.[104] As part of its Integration Team Concept, it will be critical for the Tenth Fleet MOC to be able to rapidly and effectively communicate with U.S. Cyber Command and its subordinate and fleet commands to maintain sufficient situational awareness of its networks and to be able to respond in a timely manner to any cyber threat.

In order to execute its defined mission, it is imperative that Tenth Fleet is able to exercise command and control over the Navy's networks to respond to any significant malicious network activity.[105] Especially important to this overall unity of effort will be the ability of Tenth Fleet to formulate a coherent cyber strategy that encompasses several tasks, to include the following:

> (a) Establish initial task organization and develop a plan and associated requirements for participation in the U.S. Cyber Command integration team concept.
>
> (b) Updating cyber related global operational tasks (OPTASKS) to define operational cyber force subordinate command responsibilities, tasks, and regional/global alignment.
>
> (c) Develop and implement watch certification and accreditation standards for subordinate and fleet commands.
>
> (d) Standardize reporting criteria and methods for maintaining shared situational awareness across all Tenth Fleet lines of operations and responsibilities.[106]

Without this overarching guidance passed down to subordinate and fleet commanders, it is highly likely disparate policies and guidelines will be carried out with little regard to the overall cyber effort being undertaken by Tenth Fleet, U.S. Cyber Command or its associated military components. That being said, there are several steps and measures Tenth Fleet can undertake now to ensure it maintains unity of effort, develops a strong intelligence capability and fosters tight cohesion between military and civilian scientists.

Tenth Fleet Innovation and Collaboration

Tenth Fleet is on the right track with several programs it has undertaken the past few months with regards to increased innovation and collaboration, particularly its partnerships with academic institutions, to meet the challenge of the cyber threat.

Recent engagements with the U.S. Naval War College, Carnegie Mellon University and Johns Hopkins University highlight the emphasis being placed on building a tight cohesion with academia to enhance the cyber capabilities at Fleet Cyber Command/Tenth Fleet.[107] The difficulty will be sustaining its momentum of exploring new and innovative ways to coordinate and collaborate across joint and national efforts to achieve its goal of being the preeminent cyber military organization. VADM McCullough indicated this would be a priority during the recent commissioning ceremony when he highlighted that to be able to carry out its assigned mission, Tenth Fleet needed to "work with our sister services, academia, agencies, industry, allies and partners, for the challenge is so large, to go it alone is not possible."[108] Fleet Cyber Command/Tenth Fleet is truly thinking outside of the box with civilian personnel comprising approximately 45 percent of its staff, a significant departure from the typical Navy staff.[109] Civilians add not only continuity but critical cyber expertise that is missing from our career officers who routinely change jobs and positions every two to three years. Other programs include the Cyber Federal Executive Fellowship program, which grants mid-grade officers in the Information Dominance Corps the opportunity to increase their understanding of cyber policy development and decision making at prestigious civilian research institutions.[110] There is even an outreach program to attract high school and college students by awarding four-year college Naval Reserve Officers Training Corps (NROTC) scholarships for students who demonstrate advanced cyber security skills. This newly implemented cyber-option NROTC scholarship is another key part of a comprehensive strategy to attract, recruit and develop elite cyber professionals needed to operate securely and effectively in cyber space.[111] In December 2009, the

U.S. Naval Academy in Annapolis, Maryland created the Center for Cyber Security Studies to "provide the education, resources and motivation to enable midshipmen to become effective leaders in ever-increasing cyber-enabled Navy and Marine Corps missions."[112] This new cyber security center in Annapolis is another opportunity for Tenth Fleet to take an active role in facilitating the development and nurturing of future Navy cyber warriors. One of the more innovative ideas is the outreach to civilians currently working in the cyber arena to join the naval reserves in order to build the skills and expertise of the Navy's burgeoning cyber professionals.[113]

Tenth Fleet has also made huge strides partnering with Navy, military and civilian agencies to help nurture its development to keep pace with future technological challenges. It was recently announced that the Armed Forces Communications and Electronics Association (AFCEA) Intelligence Committee and the Naval Intelligence Professionals (NIP) will host a one-day conference on 22 June 2010 to "focus on core components of the Navy's strategy for achieving information dominance and to explore how the public and private sectors can work with the Navy to ensure that it has state of the art capabilities and avoids technological surprise."[114] Program sessions will cover many issues that affect Fleet Cyber Command/Tenth Fleet, to include Intelligence, Cyber Warfare, Command and Control and Information & Knowledge Management. Attendees will include the CNO, Deputy CNO for N2/N6 (Information Dominance), and Commander U.S. Fleet Cyber Command/U.S. Tenth Fleet and senior leaders comprising the Information Dominance Corps.[115] These conferences not only foster improved information sharing but also highlight the significance of the cyber threat and positive direction the Navy is taking to lead cyber innovation and collaboration.

Recommendations for Tenth Fleet

Develop a Cyberspace Common Operational Picture (CS-COP). In order to adequately defend the Navy's computer and communication networks, Tenth Fleet needs to maintain 100 percent accountability of its networks and be able to track and respond to threats whenever and wherever needed. The National Security Agency/Central Security Service Threat Operations Center (NTOC) currently maintains a joint database for all reported incidents occurring in the military network domain.[116] However, maintaining a database of incidents doesn't address the lack of effective command and control for information assurance, which is exacerbated by the sheer magnitude of different DoD network configurations systems in existence today.[117] While NTOC makes pertinent threat information available to Tenth Fleet, there is not a single repository located inside Tenth Fleet HQ where MOC watchstanders can access this database and view the health of the Navy's, much less DoD, networks in real time. Thus, situational awareness is a fundamental problem for not only Tenth Fleet but also for DoD and DHS. More importantly, once U.S. Cyber Command is fully stood up and achieves FOC, it will be imperative that it be able to rapidly and accurately assess the status of military networks and for the individual service components, including Tenth Fleet, to be able to do the same. Tenth Fleet should take the necessary steps to track and display in real time the status of the Navy's networks and make this available to subordinate commands, fellow service cyber commands, and U.S. Cyber Command. The Navy is accustomed to tracking, displaying and disseminating friendly, neutral and enemy surface, subsurface and air contacts real-time, known as the Common Operational Picture (COP). A CS-COP would allow the Tenth Fleet MOC to better maintain situational awareness of its multiple networks and to rapidly and accurately

coordinate with U.S. Cyber Command and NTOC to report and respond to threats in a timely manner. Due to its role in computer network defense, the CS-COP would ideally be managed by NAVCYBERFOR or NCDOC to optimize threat response and mitigation; however, the important point is that Tenth Fleet must have situational awareness on the status, threats and vulnerabilities of its cyber networks at all times. This will allow Tenth Fleet to better coordinate and corroborate with other DoD and DHS cyber organizations in a timely manner to mitigate and respond to cyber threats.

Develop Well-Trained Cyber Warriors across DoD. There are two key elements that need to be addressed by Tenth Fleet to ensure it recruits, retains and develops the best cadre of cyber warriors – education and training. A common adage is that an organization is only as good as its people, and this is especially true for the military. The Navy is facing a challenge in recruiting cyber experts because of increased competition with sister services, academia, government organizations and private businesses. In order for the military to compete with other enterprises for the dwindling pool of cyber warriors, it needs to be proactive with its recruitment, education, and incentives programs to attract and retain the best talent. With each military service component conducting its own level of cyber training to meet its needs and requirements, it seems that limited resources would be better spent consolidating and enhancing those programs identified as the most effective and making them available to all DoD cyber warriors, similar to the way Air Force and Navy pilots conduct initial flight training at Pensacola Naval Air Station.[118] By coordinating and consolidating cyber training requirements, all the service components, to include Tenth Fleet, will be able to maximize the effectiveness of its cyber training program by increasing the amount of

personnel who can be trained while enhancing its organic training curriculum to meet current and future challenges. Additionally, efforts must include partnerships with civilian experts in other government enterprises (such as DHS), academia and industry to strengthen and develop the needed expertise to ensure our cyberspace security.[119] Cyber fellowships and internships within DoD and across government agencies will facilitate exchanges and ensure that cyber warriors are speaking with each other and gaining the much needed expertise to bring back to their parent organizations. Lastly, but probably the most important point, Tenth Fleet needs to ensure that every officer, sailor, Department of the Navy civilian and contractor understands the importance of the cyber mission. This entails inculcating into each person a sense of personal accountability regarding the importance to safeguard and secure our networks. The success and failure of our IA program relies ultimately on every individual strictly adhering to prescribed guidelines which outline the proper use of DoD and commercial computers, flash memory drives, e-mail usage, wireless networks, cellular phones, land-line phones, Blackberries, satellite and cable-based networks, and so forth. It is no longer adequate or sufficient for an annual online IA awareness training to prepare our Navy personnel for the cyber threat, which is present and growing. The Navy must take the time and effort to properly and effectively indoctrinate, train, inspect and hold accountable all Navy personnel regarding the established IA guidelines and policies. With the alignment of the OPNAV N2/N6 staff into a robust Information Dominance Corps, there are many skilled information professionals to augment the Tenth Fleet mission as needed.[120] Tenth Fleet will need to utilize this information dominance cadre as it will take an “all hands” effort to ensure an effective IA program fully supports the

cyber effort now and in the future for the roughly 390,000 active duty and reserve sailors which comprise the Navy.[121]

Develop Robust Exercises and Training. Tenth Fleet, via its TYCOM and regional NIOCs, should develop combined response exercises, drills and training scenarios with sister military components and civilian agencies to better respond to cyber attacks.[122] Robust cyber attacks, as delineated in Appendix B, that encompass a wide range of complexity need to be incorporated into battle exercises preparing our forces to deploy. These exercises need to mature with complexity in the same manner that our anti-surface, anti-submarine and anti-aircraft exercises are developed and executed across the inter-deployment training schedule. Our naval personnel assigned to ships, submarines, aircraft and special forces need to understand the ramifications of operating in an environment in which unfettered access to the cyberspace domain can be compromised or denied. This means that Tenth Fleet needs to coordinate closely with each of the numbered fleets and corroborate with its sister services components to support joint, NATO, coalition and Combatant Command exercise requirements. Fortunately, Tenth Fleet can utilize its Information Dominance Corps counterparts that are currently assigned to each subordinate command, fleet/squadron, ship and submarine. The Navy's best interest, as well as that of the nation, requires implementing the most realistic scenarios in the training environment.

Enhance Partnerships and Alliances with Other Agencies. Tenth Fleet cannot succeed in its mission to defend, exploit and achieve operational effects in and through cyberspace and to assure freedom of maneuver in cyberspace if it works in isolation.[123] Under the latest Quadrennial Defense Review, Defense Secretary Gates stipulated:

> DoD needs to collaborate with other U.S. departments and agencies and international partners both to support their efforts and to ensure our ability to operate in cyberspace. This mutual assistance includes information sharing, support for law enforcement, defense support to civil authorities, and homeland defense.[124]

As highlighted in the CNCI, NSSC, NMS-CO, and HSPD-7, responsibility for a federal cyber incident is dispersed across many federal departments and agencies because of the existing legal distinctions between national security and other federal networks.[125] There currently isn't legislation which requires cyber cooperation and information sharing between military and non-military agencies in the government; however, this by no means should prevent or limit Tenth Fleet from taking pro-active measures to enhance its ability to coordinate and cooperate with all entities directed to defend the GIG, be they operating under guidelines established by the NSSC or NMS-CO.[126] Simply put, Tenth Fleet needs to take steps to make certain that its subordinate commands are talking with their sister organizations in the Army, Air Force and Marine Corps. It must further ensure that close coordination and cooperation across DHS is taking place and that information sharing is as seamless as possible.

Although DHS is responsible for protecting the government and civilian networks, it will likely fall onto DoD to respond to any such attack, particularly an attack aimed at our critical infrastructure. This means that cyber entities within DHS and DoD need to clearly articulate and formalize relationships so that the U.S. can truly formulate a whole of government approach to protect our national interests in cyberspace. Even more important, particularly with the global presence of today's Navy and the large number of bases on foreign shores, the Navy must ensure it is actively pursuing increased collaboration and coordination with our allies and coalition partners. The Cooperative Defence Cyber Centre of Excellence in Tallinn, Estonia is one example of an

international effort that was developed to enhance NATO's cyber defense capability and includes Estonia, Latvia, Lithuania, Germany, Italy, the Slovak Republic, and Spain as Sponsoring Nations.[127] Fleet Cyber Command/Tenth Fleet should be very familiar with ongoing efforts at NATO and vice versa to capitalize and leverage resources expended to continually increase its understanding and comprehension of the latest developments in the cyber domain. Furthermore, there needs to be a mechanism by which best practices and policies can be leveraged and shared across the government in a timely manner to mitigate the threat to our networks. We simply cannot afford to wait for a cataclysmic cyber event to force government agencies to cooperate; the time for action is now.

Conclusion

Tenth Fleet is being stood up at an opportune time to confront the ever-growing cyber threats facing the nation. While Congress continues to debate and delay confirmation hearings for the Commander, U.S. Cyber Command, Tenth Fleet must continue to lead the way in developing and fostering innovative solutions to secure the Navy's cyber networks. Just as it did during World War II, Tenth Fleet has capitalized on many of the lessons learned in its battle to confront the U-boat threat, to include the importance of unity of effort, strong intelligence and tight cohesion between civilian scientists and military personnel. The innovative programs being undertaken with academia, civilian agencies, industry, allies and partners need to be expanded and leveraged with programs by sister service components and DHS in order to apply a truly whole of government approach that is dedicated to protecting the U.S. from cyber attack. The Navy must continue to lead from the front with its innovative programs and

partnerships and must expand its efforts to ensure we leverage the efforts being undertaken by allies and coalition partners.

Tenth Fleet needs to ensure that lessons learned, best practices and advances in firewalls and forensics technology be developed and shared a truly collaborative environment, because it makes no sense for one service to have a secure network if the rest of the DoD or DHS is vulnerable because of a failure to talk to each other. The U.S. Navy has taken the appropriate steps to counter the cyber threat with its development of the Information Dominance Corps and reconstitution of Tenth Fleet. The difficult task ahead will be to develop the synergy needed to operate in a truly collaborative, joint enterprise environment across not only DoD and DHS, but with allies and coalition partners, if we are to protect the GIG from the growing cyber threat.

Endnotes

[1] Alfred T. Mahan, "Considerations Governing the Disposition of Navies," *National Review,* July 1902, 706, quoted in George W. Baer, *One Hundred Years of Sea Power: The U.S. Navy, 1890-1990* (Stanford, CA: Stanford University Press, 1994), 14.

[2] Chief of Naval Operations Gary Roughead, "Fleet Cyber Command/Commander Tenth Fleet Implementation Plan," memorandum for Commander, U.S. Fleet Forces Command and Director of Naval Intelligence (N2), Washington, DC, July 23, 2009.

[3] Gary Roughead, "CNO Guidance for 2010: Executing the Maritime Strategy," (September 2009), 6.

[4] Commander, Fleet Cyber Command, "WARNORD: Establishment of FLTCYBERCOM and Re-establishment of U.S. Tenth Fleet," record message traffic transmitted 230007Z December 2009.

[5] Note: The U.S. Navy established Sea Frontiers on 1 July 1941 as coastal areas of defense, commencing at the shoreline and extending outwards into the sea for a nominal distance of two hundred miles. See Eliot A. Cohen and John Gooch, *The Anatomy of Failure in War: Military Misfortunes* (New York: Free Press, 1990), 59.

[6] Samuel Eliot Morison, *History of United States Naval Operations in World War II. Vol. 10: The Atlantic Battle Won* (Champaign, IL: University of Illinois Press, 1956), 13.

[7] Note: The Combined Chiefs of Staff (CCS) was formed in January 1942 and constituted the British and American Chiefs of Staff. See Rick Atkinson, *An Army at Dawn: The War in North Africa, 1942-1943* (New York: Holt, 2002), 383.

[8] Morison, *History of United States Naval Operations in World War II*, 16.

[9] Ibid., 21.

[10] Ibid.

[11] Baer, *One Hundred Years of Sea Power*, 203

[12] Montgomery C. Meigs, *Slide Rules and Submarines: American Scientists and Subsurface Warfare in World War II* (Washington, DC: National Defense University Press, 1989), 98.

[13] Nathan Miller, *War at Sea: A Naval History of World War II* (New York: Scribner, 1995), 349.

[14] Morison, *History of United States Naval Operations in World War II*, 23.

[15] Baer, *One Hundred Years of Sea Power,* 203

[16] Meigs, *Slide Rules and Submarines*, 113.

[17] Baer, *One Hundred Years of Sea Power,* 204

[18] Note: The Enigma machine was originally a commercial enciphering device developed in 1923. Messages were typed in plain text into a battery-powered device that resembled a portable typewriter, and automatically enciphered by setting the rotors of the machine. The messages could only be unscrambled if the recipient had set the rotors of his machine to the same key or setting as the sender. Germany's armed forces modified and improved the Enigma machine by adding plugs to vary the circuits, which enabled the operators to change the circuits and rotor settings every 24 hours according to a dated instruction book of keys, which presented an astronomical number of alternatives for each letter. See Miller, *War at Sea*, 94.

[19] Ibid., 350.

[20] Meigs, *Slide Rules and Submarines*, 99.

[21] Ibid., 101.

[22] Ibid., 99.

[23] Ibid., 100.

[24] Ibid., 99.

[25] Ibid., 134.

[26] Baer, *One Hundred Years of Sea Power,* 204.

[27] Cohen and Gooch, *The Anatomy of Failure in War*, 91.

[28] Shane Harris, "The Cyberwar Plan," November 14, 2009, linked from the *National Journal Magazine Homepage* at "Cover Story," http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php (accessed December 27, 2009.

[29] David Willson, "A Global Problem: Cyberspace Threats demand an International Approach," July 2009, linked from the *Armed Forces Journal Homepage* at "Past Issues: July 2009," http://www.armedforcesjournal.com/2009/07/4062667 (accessed December 27, 2009).

[30] David Elliott, "Weighing the Case for a Convention to Limit Cyber Warfare," November 2009, linked from the *Arms Control Association Homepage* at "Arms Control Today: November 2009," http://www.armscontrol.org/act/2009_11/Elliott (accessed December 27, 2009).

[31] Willson, "A Global Problem: Cyberspace Threats," July 2009.

[32] Ibid.

[33] Mark Kohlheim, "Collaborating on Cyberspace in San Diego," briefing slides, San Diego, CA, Commanding Officer, Space and Naval Warfare Systems Command, October 9, 2009.

[34] James A. Lewis, "The Korean Cyber Attacks and Their Implications for Cyber Conflict," October 23, 2009, linked from the Center for Strategic & International Studies Homepage at "Topics: Cybersecurity," http://csis.org/publication/korean-cyber-attacks-and-their-implications-cyber-conflict (accessed December 30, 2009).

[35] Larry Wortzel, "China's Cyber Offensive and How the U.S. Can Respond," *Wall Street Journal*, November 1, 2009.

[36] Elliott, "Weighing the Case for a Convention to Limit Cyber Warfare," November 2009.

[37] Note: Although no universally sanctioned DoD definitions currently exist across the cyber spectrum, there is movement towards consensus on baseline cyber definitions and types of cyber attacks. Definitions and type of attacks are briefly noted here:

Cyberspace: A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked systems and associated physical infrastructures. (Peter Pace, *The National Military Strategy for Cyberspace Operations,* 3)

Cyber Aggression: Any form of intentional harm-doing performed through electronic means; any actions by one or more individuals designed to harm others through use of computers or related peripheral equipment. (R.A. Baron and L. Peters, "New Technology Management Challenges: Hacking and Other Forms of Cyber Aggression," October 2001)

Cyber Crime: Illicit activity through an Internet connection involving unauthorized removal of data on small, portable storage devices. (Clay Wilson, "Cyber Crime," in *Cyberpower and National Security*, 416)

Cyber Espionage: Unauthorized copying or probing of a target computer's configuration to evaluate its system defenses. (Wilson, 423)

Cyber Attack: Attack conducted against cyber assets, such as software and data, carried out by means of information packets that traverse communication links; attacks can be targeted or untargeted. Some common types of attacks are listed below (US Government Accounting Office, *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*, 18):

1) **Denial of Service**: Attack from a single source that denies system access to legitimate users without actually having to compromise the targeted system. The attack overwhelms the target computer with messages and blocks legitimate traffic. (Ibid., 29)

2) **Distributed Denial of Service**: A variant of the denial-of-service attack that uses a coordinated attack from a distributed system of computers. (Ibid., 29)

3) **Logic Bombs**: A form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering action takes place. (Ibid., 29)

4) **Sniffer or Packet Sniffer**: A program that intercepts routed data and examines each packet in search of specified information. (Ibid., 29)

5) **Trojan Horse**: A program, usually disguised as a key program that a user would wish to execute, containing harmful code. (Ibid., 29)

6) **Virus**: A program that infects computer files by inserting a copy of itself into the file. A virus requires human intervention to propagate. (Ibid., 29)

7) **Worms**: A program that reproduces by copying itself from one system to another across a network. Worms do not require human intervention to propagate. (Ibid., 29)

Cyber Terrorism: A computer based attack or threat of attack intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious, or ideological; attacks should be sufficiently destructive to generate fear comparable to that from physical acts of terrorism. (Irving Lachow, "Cyber Terrorism: Menace or Myth?" in *Cyberpower and National Security*, 438).

Cyber War: Conducting, and preparing to conduct, military operations according to information-related principles, to include disrupting and/or destroying the information and communications systems of an adversary. (Irving Lachow, 438).

[38] Lewis, "The Korean Cyber Attacks," October 23, 2009.

[39] Ibid.

[40] Joseph H. Scherrer and William C. Grund, "A Cyberspace Command and Control Model," *Air War College Maxwell Papers*, no. 47 (August 2009): 4.

[41] Peter Pace, *The National Military Strategy for Cyberspace Operations* (Washington, DC: Chairman of the Joint Chiefs of Staff, December 2006), C-1.

[42] *The Council of Europe Homepage,* at "Rule of Law: Cybercrime," http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp (accessed Dec 30, 2009).

[43] *The U.S. Department of Justice: Computer Crime and Intellectual Property Section Homepage*, http://www.cybercrime.gov/intl.html#Vb (accessed January 2, 2010).

[44] *The Council of Europe Homepage* at "Rule of Law: Cybercrime - Map of the Convention's Signatory Countries," http://www.coe.int/t/dc/files/themes/cybercrime/default_en.asp (accessed Dec 30, 2009).

[45] Barack H. Obama, "Remarks by the President on Securing our Nation's Cyber Infrastructure," May 29, 2009, linked from *The Whitehouse Homepage* at "The Briefing Room," http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (accessed December 26, 2009).

[46] Barack H. Obama, "The Comprehensive National Cybersecurity Initiative," March 2, 2010, linked from the Whitehouse Homepage at "National Security Council – Cybersecurity," http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (accessed March 13, 2010).

[47] Ibid.

[48] Ibid.

[49] Ryan Singel, "White House Cyber Czar: There is No Cyberwar," *Wired*, March 4, 2010.

[50] Obama, "The Comprehensive National Cybersecurity Initiative," March 2, 2010.

[51] Ibid.

[52] Harris, "The Cyberwar Plan," November 14, 2009.

[53] George W. Bush, Homeland Security Presidential Directive/HSPD-7 (Washington, DC: The White House, December 17, 2003).

[54] Ibid.

[55] Ibid.

[56] Richard Mereand, "Securing Cyberspace: Guarding the New Frontier," *National Security Watch* 09-3 (August 2009): 5.

[57] Richard M. Crowell, "War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare," 24, linked from the U.S. Army War College DIME Homepage at "Cyberspace," http://www.carlisle.army.mil/DIME/documents/War in the Information Age - A

Primer for Cyberspace Operations in 21st Century Warfare – R M Crowell.pdf (accessed January 10, 2010)

[58] Pace, *The National Military Strategy for Cyberspace Operations,* 9.

[59] Ibid.

[60] Robert M. Gates, Quadrennial Defense Review Report (Washington, DC: U.S. Department of Defense, February 2010), 37.

[61] Sean Gallagher, "New Threat to Compel DoD to Rethink Cyber Strategy," January 22, 2010, linked from the *Defense Systems Homepage* at "Cyber Warfare," http://defensesystems.com/articles/2010/01/27/cover-story-long-cyber-march.aspx (accessed February 14, 2010).

[62] NMS-CO outlines three missions for DoD, which must be performed simultaneously: defense of the nation, national incidence response, and critical infrastructure response. See Pace, *The National Military Strategy for Cyberspace Operations,* 2.

[63] Elihu Zimet and Charles L. Barry, "Military Service Cyber Overview," in *Military Perspectives on Cyber Power*, ed. Larry K. Wentz, Charles L. Barry, and Stuart H. Starr (Washington, DC: National Defense University Press: 2009), 2.

[64] Ibid., 3.

[65] John Markoff, David E. Sanger and Thom Shanker, "In Digital Combat, U.S. Finds No Easy Deterrent," *The New York Times*, January 26, 2010.

[66] Mereand, "Securing Cyberspace," 2.

[67] ADM Gary Roughead, Chief of Naval Operations (Navy Times, October 2007), quoted in Kohlheim, "Collaborating on Cyberspace in San Diego," October 9, 2009.

[68] ADM Gary Roughead, Chief of Naval Operations, quoted in Gerry J. Gilmore, "Navy Moves to Meet Information Age Challenges," *American Forces Press Service*, October 2, 2009.

[69] Gilmore, "Navy Moves to Meet Information Age Challenges," October 2, 2009.

[70] Richard R. Burgess, "The New Main Battery: The Navy Realigns its Organization Toward Information Dominance," *Seapower*, December 2009, 16.

[71] Gary Roughead, "CNO Guidance for 2010," 6.

[72] Burgess, "The New Main Battery," 16.

[73] Chief of Naval Operations, "Establishment of the Deputy Chief of Naval Operations for Information Dominance (N2/N6)," record message traffic transmitted 292237Z October 2009.

[74] Gary Roughead, "CNO Guidance for 2010," 6.

[75] VADM Jack Dorsett, Deputy CNO for Information Dominance, quote in Chief of Naval Personnel Public Affairs, "Information Dominance Corps Warfare Insignia Approved," February 22, 2010, linked from the *United States Fleet Cyber Command/Tenth Fleet Home Page* at "Fleet Cyber/Tenth Fleet News," http://www.navy.mil/search/display.asp?story_id=51448 (accessed March 20, 2010).

[76] Chief of Naval Personnel, "Information Dominance Warfare Insignia," February 22, 2010.

[77] Mike Mullen, "Chairman of the Joint Chiefs of Staff Guidance for 2009-2010," (December 21, 2009), 4.

[78] Shaun Waterman, "U.S. Takes Aim at Cyberwarfare," *The Washington Times*, July 2, 2009.

[79] Mereand, "Securing Cyberspace," 2.

[80] Mullen, "Chairman of the Joint Chiefs of Staff Guidance 2010," 6.

[81] Mereand, "Securing Cyberspace," 3.

[82] Jeffrey A. Sorenson, "C4, Space & Cyber: Enabling the Global Network Enterprise Construct," briefing slides, Long Beach, CA, Association of the U.S. Army Symposium, May 28, 2009.

[83] Chief of Naval Operations, "Fleet Cyber Command Implementation Plan" July 23, 2009.

[84] Commander, Fleet Cyber Command, "WARNORD," 230007Z December 2009.

[85] Chief of Naval Operations, "Fleet Cyber Command Implementation Plan" July 23, 2009.

[86] Zimet and Barry, "Military Service Cyber Overview," 7.

[87] Michael A. Brown, "Navy Operations to Achieve Military Power in Cyberspace: A Draft Concept for Navy Computer Network Operations," in *Military Perspectives on Cyber Power*, ed. Larry K. Wentz, Charles L. Barry, and Stuart H. Starr (Washington, DC: National Defense University Press: 2009), 77.

[88] *U.S. Fleet Cyber Command/Tenth Fleet Homepage*, http://www.fcc.navy.mil/ (accessed 15 March 2010).

[89] Commander, Fleet Cyber Command, "WARNORD," 230007Z December 2009.

[90] Ibid.

[91] ADM Gary Roughead, Chief of Naval operations, quoted in Fleet Cyber Command/Tenth Fleet Public Affairs, "Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet," January 29, 2010, linked from the *United States Fleet Cyber Command/Tenth Fleet Home Page* at "Fleet Cyber/Tenth Fleet News," http://www.navy.mil/search/display.asp?story_id=50954 (accessed March 13, 2010).

[92] Ibid.

[93] *U.S. Fleet Cyber Command/Tenth Fleet Homepage.*

[94] VADM Barry McCullough, "U.S. Fleet Cyber Command – U.S. Tenth Fleet," briefing slides, Ft. Meade, MD, U.S. Fleet Cyber Command/U.S. Tenth Fleet, October 2010.

[95] Fleet Cyber Command, "Navy Stands Up Fleet Cyber Command," January 29, 2010.

[96] Chief of Naval Operations, "Fleet Cyber Command Implementation Plan" July 23, 2009.

[97] Note: Commander NAVCYBERFOR is dual-hatted at Commander NAVNETWARCOM. See Naval Network Warfare Command Public Affairs, "Navy Cyber Forces Established," January 26, 2010, linked from the United States Navy Homepage at "NAVNEWTWARCOM," http://www.navy.mil/search/display.asp?story_id=50853 (accessed March 22, 2010).

[98] Note: 15 regional NIOCs located throughout the US, Bahrain, Japan, and the UK: NIOC Bahrain (Bahrain), NIOC California, NIOC Denver, NIOC Florida, NIOC Georgia, NIOC Hawaii, NIOC Maryland, NIOC Menwith Hill (UK), NIOC Misawa (Japan), NIOC Suitland (MD), NIOC Texas, NIOC Virginia, NIOC Washington, NIOC West Virginia, and NIOC Yokosuka (Japan). See *The Navy CT History Homepage,* http://www.navycthistory.com/ NSGStationsHistoryDates.txt (accessed March 22, 2010).

[99] CAPT Daryl Hancock, Director of Intelligence, U.S. Fleet Cyber Command/Tenth Fleet, interview by author, January 15, 2010.

[100] VADM Barry McCullough, Commander US Fleet Cyber Command, quoted in Fleet Cyber Command, "Navy Stands Up Fleet Cyber Command," January 29, 2010.

[101] Brown, "Navy Operations to Achieve Military Power in Cyberspace," 76.

[102] Burgess, "The New Main Battery," 17.

[103] Commander, Fleet Cyber Command, "WARNORD," 230007Z December 2009.

[104] Commander, Fleet Cyber Command, "PLANORD: Establishment of FLTCYBERCOM and Re-establishment of U.S. Tenth Fleet," record message traffic transmitted 152126Z January 2010.

[105] Ibid.

[106] Ibid.

[107] Hancock, interview by author, January 15, 2010.

[108] McCullough, quoted in Fleet Cyber Command, "Navy Stands Up Fleet Cyber Command," January 29, 2010.

[109] Hancock, interview by author, January 15, 2010.

[110] Chief of Naval Operations Gary Roughead, "Cyber Federal Executive Fellowship Program," OPNAV Instruction 1500.79, Washington, DC, May 7, 2009.

[111] Naval Service Training Command Public Affairs, “Navy Offers Four-Year NROTC Scholarships to Winners of Cyber Challenge,” March 5, 2010, linked from the *United States Fleet Cyber Command/Tenth Fleet Home Page* at “Fleet Cyber/Tenth Fleet News,” http://www.navy.mil/search/display.asp?story_id=51745 (accessed March 15, 2010).

[112] *The US Naval Academy Center for Cyber Security Studies Homepage*, http://www.usna.edu/cyber/index.php (accessed March 22, 2010).

[113] Hancock, interview by author, January 15, 2010.

[114] *The Armed Forces Communications and Electronics Association Homepage*, http://www.afcea.org/events/NavyDay/welcome.asp (accessed March 15, 2010).

[115] Ibid.

[116] Mike Mullen, “Chairman of the Joint Chiefs of Staff Instruction: Information Assurance (IA) and Computer Network Defense (CND),” (August 12, 2008), B-8.

[117] Gallagher, “New Threat to Compel DoD to Rethink Cyber Strategy,” January 22, 2010.

[118] Bruce D. Caulkins, “Proactive Self-Defense in Cyberspace,” *The Land Warfare Papers*, no. 72 (August 2009): 11.

[119] Bruce L. Meyer, “Defending the New Silk Road,” *Armed Forces Journal*, September 2009, 35.

[120] Roughead, quoted in Gilmore, “Navy Moves to Meet Information Age Challenges,” October 2, 2009.

[121] Frank A. DiStasio, Jr., “The Department of defense Budget,” in Fiscal Year 2010 Army Budget - An Analysis (Arlington, VA: Association of the U.S. Army, 2009), 34.

[122] Meyer, “Defending the New Silk Road,” 35.

[123] Barack H. Obama, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (Washington, DC: The White House, May 2009), iv.

[124] Gates, Quadrennial Defense Review, 39.

[125] Obama, Cyberspace Policy Review, 23.

[126] Caulkins, “Proactive Self-Defense in Cyberspace,” 11.

[127] *The Cooperative Cyber Defence Centre of Excellence Homepage*, http://www.ccdcoe.org/ (accessed March 15, 2010).