NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE ARMED
SERVICES COMMITTEE

Statement of

VADM BERNARD J. McCULLOUGH, III

Commander, United States Fleet Cyber Command

Before the

Terrorism and Unconventional Threats and Capabilities Subcommittee

of the House Armed Services Committee

Digital Domain: Organize the Military Departments for Cyber

Operations

September 23, 2010

NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE ARMED
SERVICES COMMITTEE

Chairwoman Sanchez, Ranking Member Miller and distinguished members of the Subcommittee, thank you for the opportunity to discuss the United States Fleet Cyber Command and TENTH Fleet.

Madame Chairwoman, on January 29, 2010, I assumed command of the United States Fleet Cyber Command and United States Navy TENTH Fleet. As the Navy's Component Command to United States Cyber Command, and an Echelon Two Navy Command, subordinate to the Chief of Naval Operations, Fleet Cyber Command directs cyberspace operations in defense and support of our forces to deter and defeat aggression and ensure freedom of action. While much of our mission parallels those of the other Services' cyber components, Fleet Cyber Command has unique responsibilities as the central operational authority for networks, cryptology, signals intelligence, information operations, cyber, electronic warfare and space in support of forces afloat and ashore. The Navy's vision is to fully develop our ability to operate in cyberspace by fusing old – and developing new – capabilities and capacities across our networks, signal intelligence systems, and electronic warfare systems. As such, we organize and direct Navy cryptologic operations worldwide and integrate information operation and space planning and operations as directed.

*History*

TENTH Fleet was established during World War II to develop and implement anti-submarine warfare in the Atlantic Ocean. At that time, we faced a threat much improved in capability and capacity over those possessed in World War I. This threat had enormous game changing potential. TENTH Fleet, which had no permanently assigned ships, defeated the German Submarine threat through integration of intelligence and the development of advanced

tactics, techniques, and procedures. Today, the re-established TENTH Fleet is built upon the same principles. We conduct operations, with information warfare specialists, intelligence specialists, cryptologic and electronic warfare specialists, and traditional war fighters, to ensure freedom of maneuver against an advanced, game changing threat. The operational focus of Fleet Cyber Command will enable us to immediately respond to threats on our networks and maintain information assurance for our Navy. This operational framework allows us to accomplish our mission for defense of our network operations.

To succeed on the modern battlefield we must be able to operate freely across the electronic spectrum defeating threats that range from the mundane, such as atmospheric interference, to the highly advanced, such as network intrusion and malicious attack. It is Fleet Cyber Command's responsibility to analyze this advanced threat and develop the tactics, techniques and procedures necessary to defend our network and ensure our freedom of operation.

*Structure*

The Navy is operationally dynamic and our networks are complicated by distance and time. The Navy not only has Sailors stationed across the earth's oceans, but is also supporting ground operations in Afghanistan, Iraq, and many other locations around the globe. We currently have more than 10,000 sailors involved in these ground operations.

Fleet Cyber Command is a global command with locations around the world able to maintain and operate networks both ashore and afloat, guaranteeing our ability to conduct full spectrum cyber operations wherever our mission takes us. With Commander U.S. TENTH Fleet as the operational level commander, our structure is built around a typical Navy Task Force

Organization. This structure assigns regional responsibilities to subordinate task groups and provides support for specific cryptologic requirements. This Task Force Organization allows for a diverse dissemination of intelligence, technology and responsibilities and provides us with the ability to respond quickly to tasking in support of fleet requirements. It also facilitates our interaction with U.S. Cyber Command and service cyber components at the local level. We have continued to develop a robust structure within our Task Forces that will continue to provide rapid direct support across the spectrum of operations.

Navy network operations are provided by Network Warfare Command (CTF1010). Its subordinate units include Naval Computer and Telecommunications Area Master Station (NCTAMS) Atlantic and Pacific, which provide network direction, maintenance and shore based relay to the Fleet. Network defense is performed by Navy Cyber Defense Operation Command (CTF 1020). This organization works to detect network threats and to secure network responses.

Our information operations are overseen by the Navy Information Operation Command (NIOC) Norfolk (CTF 1030), with detachments in San Diego and Whidbey Island. Fleet and Theater operations are coordinated through NIOC Texas (CTF 1040), NIOC Georgia (CTF 1050), NIOC Maryland (CTF 1060), NIOC Colorado (CTF 1080) and their subordinate commands located around the world. Our cryptologic component operations are maintained at these locations under the CTF1000 structure.

CTF 1090 (Naval Information Operation Center Suitland) is established as our research and development group. It is tasked with developing technologies that are ready-to-field in response to supported Fleet and Joint tasking.

External and internal organization charts are included for your review.

None of our efforts will provide mission accomplishment without effective recruiting and training of Sailors who possess the technological acumen and the ability to apply their skills to the defense of the Fleet's networks. I have visited all but one of my operational commands, and I can assure the sub-committee that the Navy has an outstanding force of Sailors ready to support the Nation across the entire range of cyber operations. Given the dynamic nature of the cyberspace domain, we must continue to evolve our force. We have initiatives to create new officer specialties including cyber Engineers and Warrant Officers. The establishment of a cyber curriculum at the United States Naval Academy will create new opportunities to educate the officers who will command Naval cyber components and capabilities.

*Mission*

As Fleet Cyber Command continues to mature, we are finding ways to capitalize on the expertise of our sister Services. As a supporting command to U.S. Cyber Command, we are using the commonalities between service components to build a network defense-in-depth architecture, allowing our diverse capabilities to create robust and adaptable global cyber defense. If one service discovers, analyzes and defeats a threat, that information can be rapidly disseminated to the other Services to minimize any intrusion effort and create a unified response.

Operationally we are moving out. Since our standup in January, we have partnered with U.S. Cyber Command's Service components in support of United States Pacific Command and Pacific Fleet exercises. We are reviewing our network operations to enhance shared situational awareness and the inherent security that comes from cooperative oversight. We have also partnered with industry, academia, and Federally Funded Research and Development Centers to

take advantage of their knowledge and capability. The commercial sector drives this domain and we must leverage their capacity and investment.

Coordination across domains is critical. Efforts to secure one system or provide a network defense must be coordinated to prevent unintentional interference with friendly systems. From navigational systems, to internet access and from the EA-18G Growler aircraft to shipboard SLQ-32 jammers, TENTH Fleet is working quickly to integrate with and complement the mission requirements of the other numbered Fleets and geographical Navy component commanders. The cooperation between Fleet staffs, is one of the key concepts behind TENTH Fleet's effort and one of the reasons for our rapid initial success.

My staff and command headquarters at Ft. Meade are growing in strength and capacity each month. We currently operate with a headquarters staff of 130 that will grow to approximately 200 billets over the next few years. The staffing rate ensures that our command will acquire not only technologically skilled Sailors, but also those who have a wealth of operational experience that they can draw from as we face the myriad challenges associated with cybersecurity.

Some of these challenges include: developing and maintaining a mindset that views the Network as an operational space; providing support across the Services to maintain our freedom of maneuver within cyberspace; developing cyber operations as a functional area, and creating a detailed concept of operations.

As we continue our operational development, we will be able to better support Fleet and Joint Exercises, which will provide required feedback on our ability to operate in a denied or

contested cyber environment. This feedback is critical to enable us to assess and improve our capabilities to support freedom of operations in the face of ever adapting threats. These future threats are not just faced by Navy or DOD systems, but can affect civilian users as well, and they may come from non-traditional sources. Non-state actors, will no doubt, seek greater capability to affect our networks, and as a Nation, we must be ready to challenge this asymmetric threat.

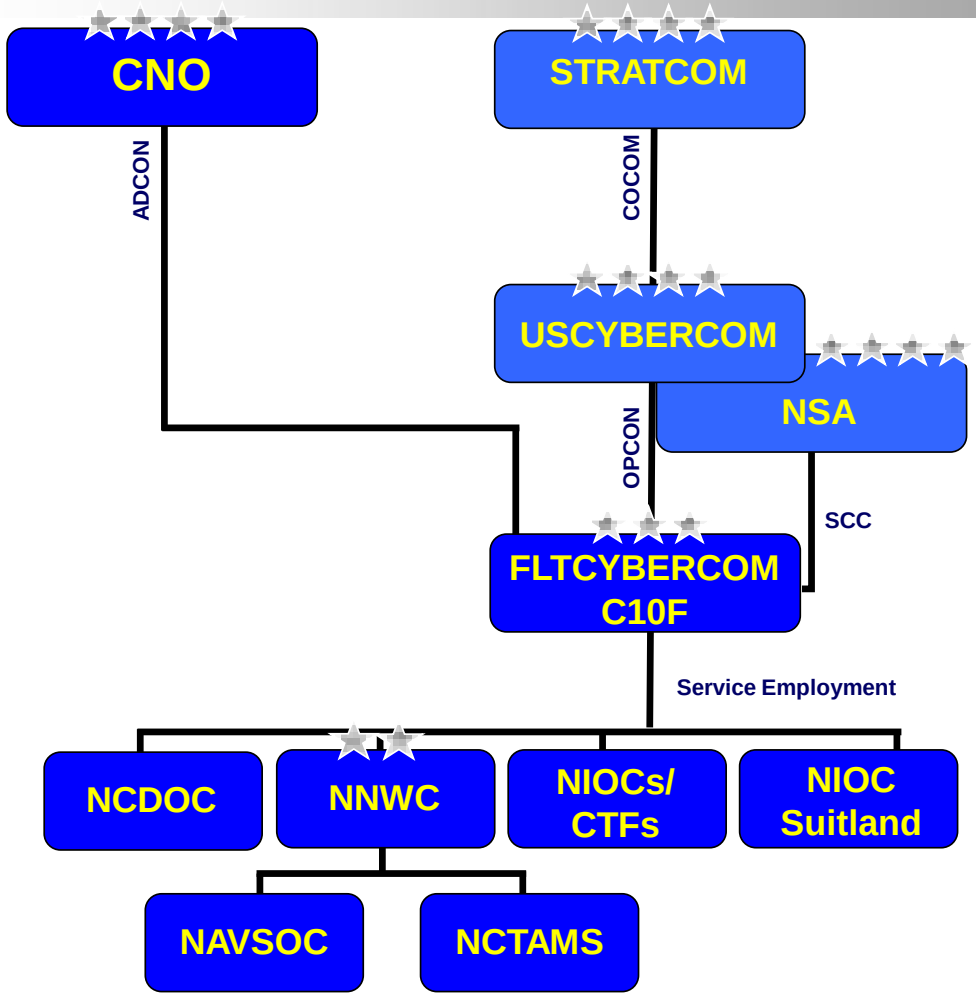
U.S. Fleet Cyber Command is also the Navy's operational authority on Electronic Warfare and Electromagnetic Spectrum Operations. In conjunction with the other Services, we are working to develop a comprehensive joint electromagnetic spectrum operation plan to ensure that our networks can operate within a spectrum in which maneuver space is restricted not only by adversary and competitor, but also by the expanding commercial enterprise allotment of radio frequency bands. The sheer number of radio frequency users proves that it is not enough to be able to defend ourselves from kinetic and directed network attacks, but we must be able to secure our network operations that take place over the air.

Every day, I am amazed at the ability of our Sailors to think beyond the traditional areas and to apply their expertise to the cyber realm. It is that environment that we will cultivate and use to help recruit future experts. There is no way the Defense Department can compete with industry in the area of monetary compensation, but we can provide our people expanded opportunities for education and training and help them build experience as leaders that cannot be obtained elsewhere.

With the cooperation of industry partners, Federally Funded Research and Development centers throughout the DOD, and academia, we will be able to better assess, understand and respond more rapidly to a wider variety of threats.

I thank you for this opportunity to present the U.S. Fleet Cyber Command and TENTH Fleet, and appreciate your support of our Navy and the Department of Defense. I look forward to answering your questions.

# External C2 Relationships



# C10F Standing Task Organization