United States Government Accountability Office

GAO

Report to Congressional Requesters

May 2011

DEFENSE DEPARTMENT CYBER EFFORTS

More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities

GAO-11-421

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAY 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defense Department Cyber Efforts: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Government Accountability Office,441 G Street NW,Washington,DC,20548**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**35**	

May 2011

DEFENSE DEPARTMENT CYBER EFFORTS

More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-11-421, a report to congressional requesters

Why GAO Did This Study

The U.S. military depends heavily on computer networks, and potential adversaries see cyberwarfare as an opportunity to pose a significant threat at low cost—a few programmers could cripple an entire information system. The Department of Defense (DOD) created U.S. Cyber Command to counter cyber threats, and tasked the military services with providing support. GAO examined the extent to which DOD and U.S. Cyber Command have identified for the military services the (1) roles and responsibilities, (2) command and control relationships, and (3) mission requirements and capabilities to enable them to organize, train, and equip for cyberspace operations. GAO reviewed relevant plans, policies, and guidance, and interviewed key DOD and military service officials regarding cyberspace operations.

What GAO Recommends

GAO recommends that DOD set a timeline to develop and publish specific guidance regarding U.S. Cyber Command and its service components' cyberspace operations, including: (1) categories of personnel that can conduct various cyberspace operations; (2) command and control relationships between U.S. Cyber Command and the geographic combatant commands; and (3) mission requirements and capabilities, including skill sets, the services must meet to provide long-term operational support to the command. DOD agreed with the recommendations.

View GAO-11-421 or key components. For more information, contact Davi M. D'Agostino at (202) 512-5431 or dagostinod@gao.gov.

What GAO Found

DOD and U.S. Cyber Command have made progress in identifying the roles and responsibilities of the organizations that support DOD cyberspace operations, but additional detail and clarity is needed. GAO's analysis of U.S. Cyber Command's November 2010 *Concept of Operations* showed that it generally meets joint guidance and maps out U.S. Cyber Command's organizational and operational relationships in general terms. However, greater specificity is needed as to the categories of personnel that can conduct various types of cyberspace operations in order for the military services to organize, train, and equip cyber forces. The services may use military, civilian government, and contractor personnel to conduct cyberspace operations, and U.S. Cyber Command's *Concept of Operations* describes general roles and responsibilities for cyberspace operations performed by U.S. Cyber Command's directorates, the military services, and the respective service components. However, service officials indicated that DOD guidance was insufficient to determine precisely what civilian activities are permissible for certain cyber activities, that DOD is still reviewing the appropriate roles for government civilians in this domain, and that the military services may be constrained by limits on their total number of uniformed personnel, among other things. Without the specific guidance, the services may in the future have difficulty in meeting personnel needs for certain types of cyber forces.

U.S. Cyber Command's *Concept of Operations* generally describes the command and control relationships between U.S. Cyber Command and the geographic combatant commands, but additional specificity would enable the military services to better plan their support for DOD cyberspace operations. DOD guidance calls for command and control relationships to be identified in the planning process. The *Concept of Operations* recognizes that a majority of cyberspace operations will originate at the theater and local levels, placing them under the immediate control of the geographic combatant commanders and requiring U.S. Cyber Command to provide cyberspace operations support. However, officials from the four military services cited a need for additional specificity as to command and control relationships for cyberspace operations between U.S. Cyber Command and the geographic combatant commands, to enable them to provide forces to the appropriate command. DOD recognizes this challenge in command and control and is conducting exercises and studies to work toward its resolution.

U.S. Cyber Command has made progress in operational planning for its missions but has not fully defined long-term mission requirements and desired capabilities to guide the services' efforts to recruit, train, and provide forces with appropriate skill sets. DOD guidance requires that combatant commanders provide mission requirements the services can use in plans to organize, train, and equip their forces. However, GAO determined that in the absence of detailed direction from U.S. Strategic Command, the services are using disparate, service-specific approaches to organize, train, and equip forces for cyberspace operations, and these approaches may not enable them to meet U.S. Cyber Command's mission needs.

Contents

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

May 20, 2011

Congressional Requesters

The U.S. military is highly dependent on communications and on computer networks—its Global Information Grid—which are potentially jeopardized by the millions of denial-of-service attacks, hacking, malware, bot-nets, viruses, and other intrusions that occur on a daily basis. As we have stated in prior work,[1] the threat to Department of Defense (DOD) computer networks is substantial and the potential for sabotage and destruction is present. Potential adversaries recognize that cyberspace is an asymmetric means to counter U.S. military power, particularly since cyberwarfare poses a significant threat at a low cost—that is, a handful of programmers could cripple an entire information system. In February 2011, the Deputy Secretary of Defense said that more than 100 foreign intelligence agencies have tried to breach DOD computer networks and that one was successful in breaching networks containing classified information.[2] Also, the President of the United States has identified this threat as one of the most serious national security challenges facing the nation.

Cyber threats constitute an emerging mission area for DOD, and DOD's role in broader U.S. government cyberspace efforts is still evolving. To assist in its efforts to counter cyberspace threats, DOD directed the establishment of U.S. Cyber Command in 2009 as a subunified command under U.S. Strategic Command. Further, each of the military services was required to identify appropriate component support for U.S. Cyber Command, and to have that support in place and functioning before U.S. Cyber Command reached full operating capability, which occurred in October 2010. Much like its parent command, U.S. Cyber Command is attempting to better meet the security challenges of the new century and effectively anticipate, counter, and eliminate the emergence of cyber threats at home and overseas, just as its counterparts strive to do in the air, land, sea, and space domains.

Since 2008, at the request of this subcommittee, we have conducted two reviews, the first focused on the federal government's Comprehensive

[1] GAO classified report from May 2010 on challenges to DOD's cyber efforts.

[2] Deputy Secretary of Defense William J. Lynn, III, Remarks on Cyber at the RSA Conference, February 15, 2011.

National Cybersecurity Initiative and the second on DOD's cyberspace capabilities.[3] At your request, this review examined the extent to which the services are prepared to conduct cyberspace operations in support of U.S. Cyber Command. Specifically, this report focuses on the extent to which DOD and U.S. Cyber Command have identified for the military services (1) roles and responsibilities including categories of personnel that can conduct various cyberspace operations; (2) command and control relationships, to include the geographic combatant commands; and (3) mission requirements and capabilities in support of U.S. Cyber Command to enable them to organize, train, and equip for cyberspace operations.

To address our objectives, we reviewed and analyzed DOD, U.S. Strategic Command, U.S. Cyber Command, Army, Navy, Marine Corps, and Air Force plans, policies, and guidance regarding military operations in cyberspace. We met with cognizant officials in the Office of the Secretary of Defense, the Joint Staff, U.S. Strategic Command, U.S. Cyber Command and its service components, and the National Security Agency to discuss the progress made in establishing U.S. Cyber Command and providing guidance to the military services for their cyberspace activities. Additionally, we met with officials from the Army, Navy, Marine Corps, and Air Force, both from headquarters and from various service training commands, to discuss the steps they have taken to establish support to U.S. Cyber Command and to identify how they have incorporated any DOD-wide or U.S. Cyber Command guidance into the development of their respective cyberspace capabilities, specifically with regard to staffing and training cyberspace personnel. Additional information on our scope and methodology appears in appendix I.

We conducted this performance audit from May 2010 to May 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[3] GAO, *Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative*, GAO-10-338 (Washington, D.C.: Mar. 5, 2010). We also issued a classified report in May 2010 on challenges to DOD's cyber efforts.

Background

As with other joint commands, U.S. Cyber Command operates and is structured according to joint DOD doctrine and guidance. DOD's Joint Publication 1 states that a subunified command, such as U.S. Cyber Command, has functions and responsibilities similar to those of the commanders of unified commands, and exercises operational control of assigned commands and forces and, normally, over attached forces within the assigned joint operations area or functional area.[4] Within this command structure, subunified commands are responsible for operational planning for their missions. Guidance for developing such plans is provided by DOD's joint operation planning process.[5] This process establishes objectives, assesses threats, identifies capabilities needed to achieve the objectives in a given environment, and ensures that capabilities (and the military forces needed to deliver those capabilities) are allocated to achieve mission success. Joint operation planning and execution procedures also include assessing and monitoring the readiness of those units providing the capabilities for the missions they are assigned. Overall, the purpose of joint operation planning is to reduce the risks inherent in military operations. The commanders of military service components of subunified commands also have responsibilities that derive from their roles in fulfilling the services' support function, such as the development of program and budget requests, and the provision of supporting plans and data on service forces to the subunified command. Additionally, they are responsible for maintaining internal administration and discipline and communications with both their subunified commander and their service chief.

In June 2009, the Secretary of Defense issued a memorandum directing the creation of U.S. Cyber Command as a subunified command to U.S. Strategic Command, and requiring the military departments to identify and provide appropriate component support to U.S. Cyber Command, and to have this support in place and functioning prior to the new subunified command's reaching full operating capability. The memo required U.S. Cyber Command to focus on integration of cyberspace operations and possess the technical capability to address the risk of cyber threats and vulnerabilities and secure freedom of action in cyberspace. The memo further called for U.S. Cyber Command to "synchroniz[e] warfighting effects across the global security environment," as well as support civil

[4] Joint Chiefs of Staff, Joint Publication 1: *Doctrine for the Armed Forces of the United States* (May 2, 2007, incorporating Change 1, Mar. 20, 2009).

[5] Joint Chiefs of Staff, Joint Publication 5-0: *Joint Operation Planning* (Dec. 26, 2006).

authorities and international partners. The Director of the National Security Agency was also subsequently designated to hold the position of Commander of U.S. Cyber Command.

Following its authorization in June 2009, U.S. Cyber Command reached its initial operating capability on May 21, 2010, and was declared to be at full operating capability[6] on October 31, 2010. U.S. Cyber Command is organized with various joint staff directorates corresponding to the major functions of command, such as personnel, intelligence, operations, logistics, plans, and communications systems. It is supported by the Defense Information Systems Agency which, among other things, is responsible for designing, provisioning, operating, and maintaining certain DOD classified and unclassified networks. Additionally, U.S. Cyber Command receives infrastructure, security, information assurance, and various other forms of support from the National Security Agency. See figure 1 for a diagram of U.S. Cyber Command's organizational structure. This new command has identified three lines of operation: DOD Global

[6] In an October 1, 2010 memorandum, the Commander of U.S. Cyber Command defined full operational capability for his command as the completion of the following critical tasks: establishing a single, integrated Joint Operations Center; supporting cyber planning for combatant commanders; acquiring sufficient resources (personnel, information technology, and logistics); transitioning the Joint Task Force-Global Network Operations to Fort Meade, Maryland; and developing service component roles and responsibilities and integrating forces. The Deputy Secretary of Defense confirmed this and declared that U.S. Cyber Command had reached full operational capability in a memorandum dated October 31, 2010.

Information Grid operations,[7] defensive cyberspace operations,[8] and offensive cyberspace operations.[9] DOD Global Information Grid operations consists of network operations to preserve availability, integrity, authentication, confidentiality, and non-repudiation of information on DOD networks, a mission that the services have been conducting since the 1990s. Defensive cyberspace operations builds upon the concept of computer network defense, while adding an operational aspect for U.S. Cyber Command, referred to as Dynamic Network Defense Operations.[10] Offensive cyberspace operations is a newly defined line of operation for U.S. Cyber Command which is focused on taking actions and achieving outcomes in cyberspace to meet national or DOD objectives.

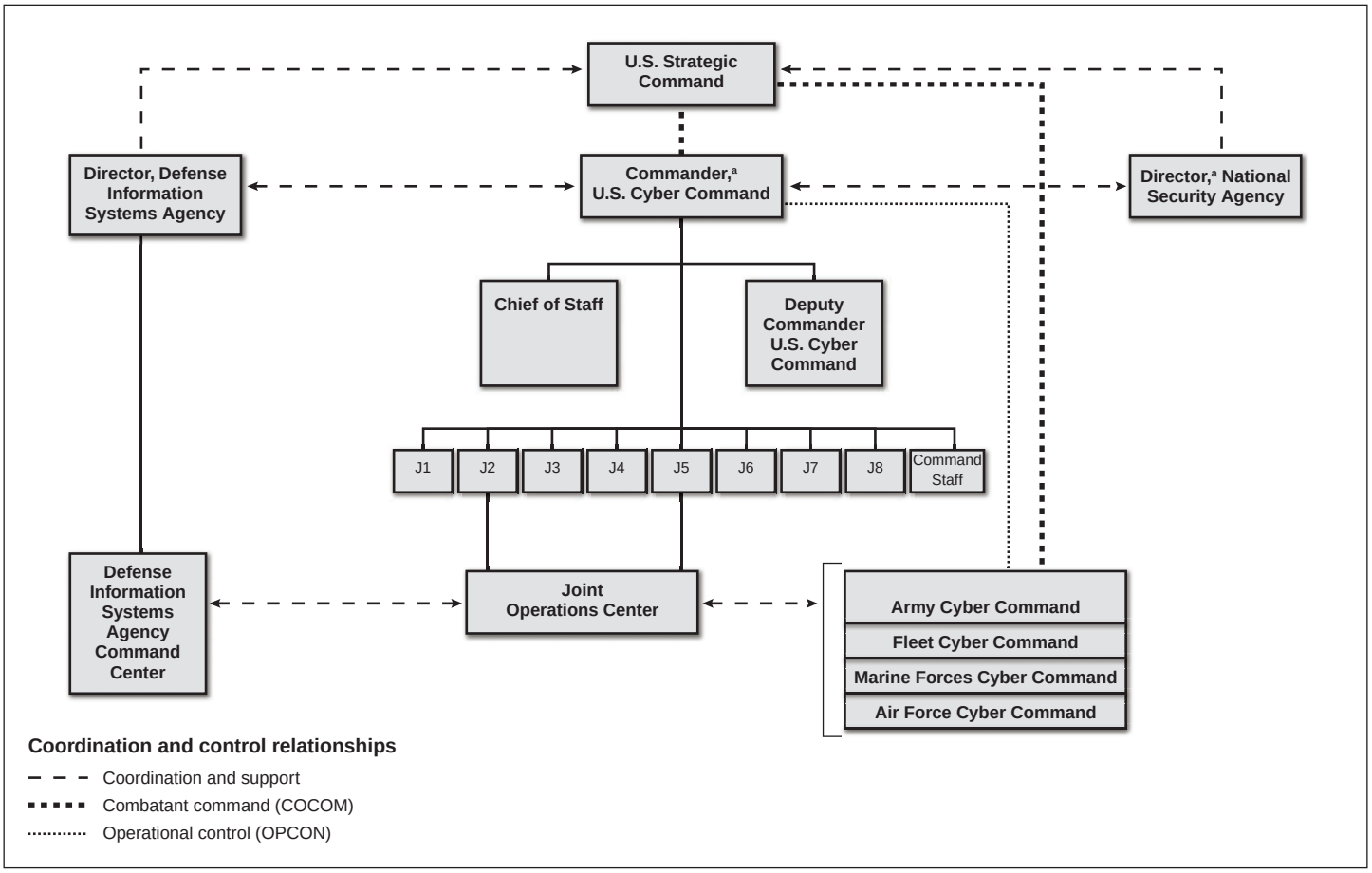
[7] DOD Global Information Grid operations are actions taken to direct, and provide guidance and unity of effort to support efforts to design, build, configure, secure, operate, maintain, and sustain DOD networks to create and preserve availability, integrity, authentication, confidentiality and non-repudiation of information. Proactive Network Operations, the major operational method by which U.S. Cyber Command will conduct this line of operation, anticipates vulnerabilities and takes actions to preserve availability, confidentiality, integrity, and non-repudiation prior to the discovery of threats and intrusions. U.S. Cyber Command, *USCYBERCOM Concept of Operations*, Version 1.0 (Sept. 21, 2010).

[8] Defensive cyberspace operations direct and synchronize actions to detect, analyze, counter, and mitigate cyber threats and vulnerabilities; to outmaneuver adversaries taking or about to take offensive actions; and to otherwise protect critical missions that enable U.S. freedom of action in cyberspace. This line of operation can trigger offensive cyberspace operations or other response actions necessary to defend DOD networks in response to hostile acts, or demonstrated hostile intent. Dynamic Network Defense Operations, the key U.S. Cyber Command operational method for defensive cyberspace operations, are those machine-synchronized and other actions to rapidly detect, analyze, counter and mitigate threats and vulnerabilities to DOD information networks. This line of operation is informed by timely intelligence, threat indicators, vulnerability information, and effects assessment information from the other lines of operation. U.S. Cyber Command, *USCYBERCOM Concept of Operations*, Version 1.0.

[9] Offensive cyberspace operations are the creation of various enabling and attack effects in cyberspace, to meet or support national and combatant commander's objectives and to actively defend DOD or other information networks, as directed. The primary U.S. Cyber Command offensive operational method will be effects-based operational planning and execution, maximizing leveraging and coordination across DOD and the interagency to meet objectives. Offensive targeting will be conducted using the guidance, apportionment, and tasking process. U.S. Cyber Command, *USCYBERCOM Concept of Operations*, Version 1.0.

[10] See footnote 8 for the definition of Dynamic Network Defense Operations in U.S. Cyber Command's *Concept of Operations*.

Figure 1: U.S. Cyber Command



Source: GAO analysis of DOD documentation.

[a]The Commander, U.S. Cyber Command, also holds the position of Director, National Security Agency.

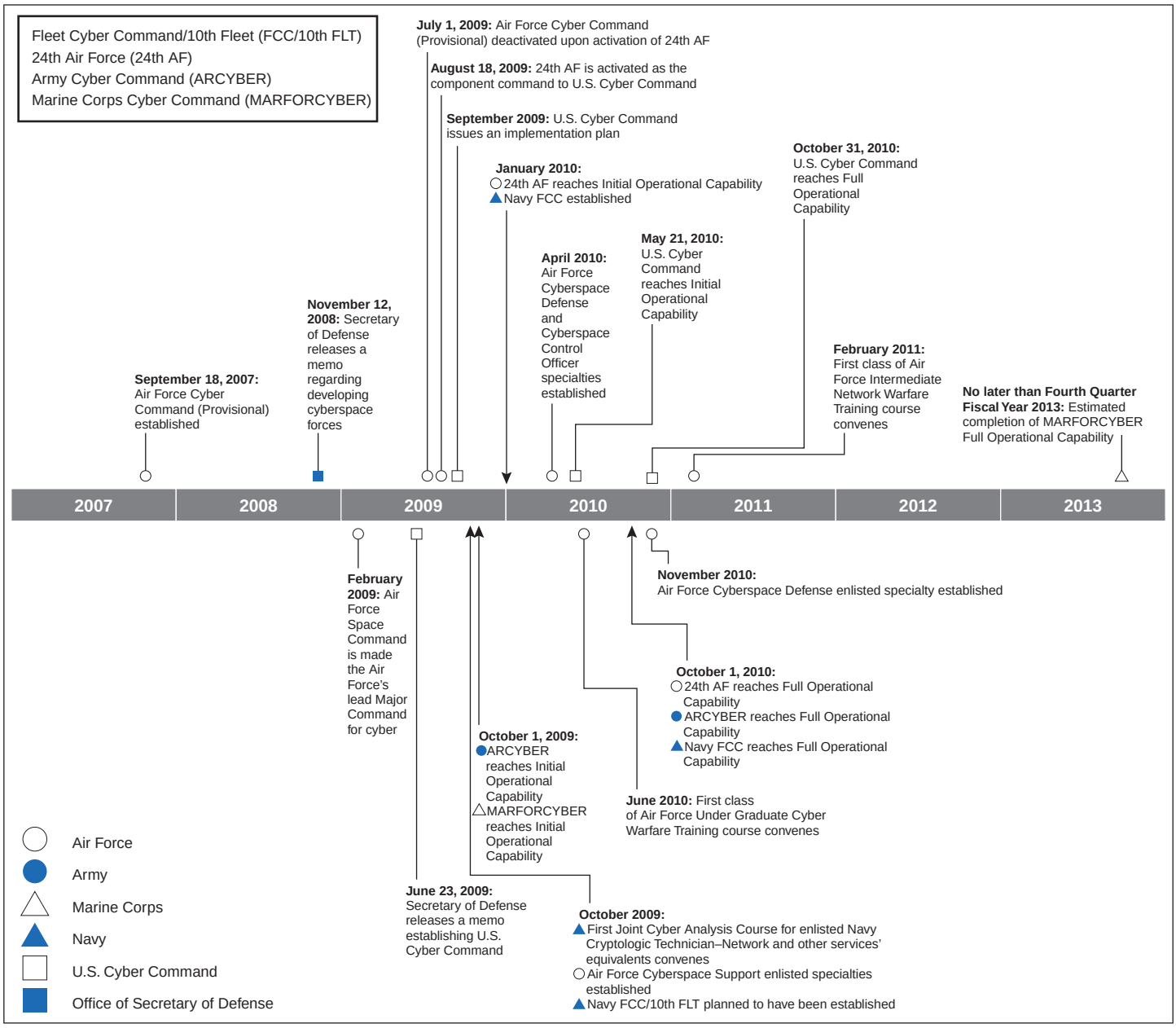
As directed by the Secretary of Defense in June 2009, each of the military departments provides service components for cyberspace operations to U.S. Cyber Command: Army Cyber Command; Fleet Cyber Command; Marine Forces Cyber Command; and Air Force Cyber Command. Three of the four service components—Army, Navy, and Air Force—all declared full operational capability in October 2010. However, officials with Marine Forces Cyber Command have stated that while they are currently capable of conducting missions, they are still in the process of establishing the command and will not reach full operational capability until the latter half of 2013. Officials and documentation from the Army, Navy, Marine Corps, and Air Force showed us that they have all retained administrative control

over their cyber service components. The Secretary of Defense assigned combatant command authority over the cyber service components to U.S. Strategic Command, which then delegated operational control over the cyber service component commands to U.S. Cyber Command.[11]

The military services developed their service component commands in response to direction from the Secretary of Defense's June 2009 memo, but DOD had already recognized the importance of the cyberspace domain. For example, beginning in late 2007, the Air Force attempted to develop its own service-specific cyber command, though the Air Force later gave the cyberspace operations mission to Air Force Space Command and Air Force Cyber Command. Also, in November 2008, the Secretary of Defense directed the military services to leverage the Navy's existing computer network operations training facilities in order to fulfill the anticipated need for more cyberspace operators. Figure 2 presents a timeline of milestones related to the establishment of U.S. Cyber Command and other cyberspace operations–related events.

[11] DOD defines administrative control as the direction or exercise of authority over subordinate organizations in respect to administration and support, including organization of service forces, control of resources and equipment, personnel management, unit logistics, individual and unit training, readiness, mobilization, demobilization, discipline, and other matters not included in the operational missions of the subordinate or other organizations. The definition of operational control includes the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Joint Chiefs of Staff, Joint Publication 1-02: *Department of Defense Dictionary of Military and Associated Terms* (Nov. 8, 2010, as amended through Dec. 31, 2010).

Figure 2: DOD Cyberspace Operations Timeline



Source: GAO analysis of DOD documentation.

As DOD's role in the emerging domain of cyberspace has evolved, so have the various key terms and definitions related to cyberspace operations. As we previously reported, DOD needs more comprehensive doctrine and

common definitions for cyberspace operations, and we recommended that DOD revise its existing body of joint doctrine to include complete and up-to-date cyberspace-related definitions while it is deciding whether to add a dedicated joint doctrine for cyberspace operations.[12] As of February 2011, DOD has defined numerous key cyber-related terms (see table 1 for a list of some of those definitions), however, other and newer terms—such as DOD Global Information Grid operations, defensive cyberspace operations, and offensive cyberspace operations discussed above—have not yet been added to DOD's joint dictionary.[13]

Table 1: DOD Cyberspace-Related Terms and Definitions

Term	Definition
Cyberspace	A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
Cyberspace Operations	The employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid.
Computer Network Attack (CNA)	Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.
Computer Network Exploitation (CNE)	Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.
Computer Network Defense (CND)	Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks.
Computer Network Operations (CNO)	Comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations.
Global Information Grid (GIG)	The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The Global Information Grid includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and National Security Systems.

[12] GAO classified report from May 2010 on challenges to DOD's cyber efforts.

[13] Joint Pub. 1-02 (Nov. 8, 2010, as amended through Dec. 31, 2010).

Term	Definition
Information Assurance (IA)	Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
Network Operations (NETOPS)	Activities conducted to operate and defend the Global Information Grid.

Source: Joint Chiefs of Staff, Joint Publication 1-02: *Department of Defense Dictionary of Military and Associated Terms* (Nov. 8, 2010, as amended through Dec. 31, 2010).

DOD and U.S. Cyber Command Have Broadly Identified Roles and Responsibilities for Cyberspace Operations, but Additional Clarity Is Needed

DOD and U.S. Cyber Command have made progress in identifying the roles and responsibilities of the various organizations that support DOD cyberspace operations. Our analysis showed that U.S. Cyber Command's *Concept of Operations* generally meets joint guidance, but a greater level of detail is needed with regard to the categories of personnel—military, government civilian, or civilian contractor—that may conduct cyberspace operations in order for the military services to organize, train, and equip operations forces. Title 10 of the U.S. Code and DOD directives and guidance implementing this authority[14] identify overall roles and responsibilities for the military services and combatant commands. These documents delineate the functions of the military services, including organizing, training, equipping, and providing cyberspace forces, as well as meeting the operational requirements of the combatant commands. They also delineate the functions of a combatant command, including giving authoritative direction to subordinate commands and forces necessary to carry out missions assigned to the command, organizing and employing forces to carry out missions assigned to the command, and assigning command functions to subordinate commanders. These documents also define the relationships between combatant commanders, including "supporting" and "supported" relationships, and the authority for a combatant commander to establish and delegate certain responsibilities to a subunified commander. Additionally, the 2008 *Unified Command Plan* assigns to U.S. Strategic Command the responsibility for synchronizing the planning of cyberspace operations. This responsibility was delegated to U.S. Cyber Command upon its establishment by the Secretary of Defense in June 2009.

[14] DOD Directive 5100.01: *Functions of the Department of Defense and Its Major Components* (Dec. 21, 2010), and Joint Pub. 1 (May 2, 2007, incorporating Change 1, Mar. 20, 2009).

U.S. Cyber Command has developed a *Concept of Operations*. The document, signed by the Commander of U.S. Cyber Command in September 2010 and released in November 2010, lays out broad roles and responsibilities for cyberspace operations and our evaluation showed that it generally meets joint guidance. Joint guidance calls for a concept of operations to include, among other things, the following actions: state the commander's intent; describe the central approach the joint force commander intends to take to accomplish the mission; provide for the application, synchronization, and integration of forces and capabilities in time, space, and purpose; focus on friendly and adversary Centers of Gravity, and their associated critical vulnerabilities; and relate the joint force's objectives and desired effects to those of the next higher command and other organizations as necessary.[15] The *Concept of Operations* states in its commander's intent section that the Commander of U.S. Cyber Command's top priorities include the following: improving the security and defense of U.S. military networks, maturing U.S. Cyber Command, working with the services to build the cyber force, and collaborating with partners. Additionally, the *Concept of Operations* states that U.S. Cyber Command will exercise control of assigned and attached forces to operate and defend DOD networks as well as conduct offensive cyberspace operations, as directed. It further states that the services retain primary responsibility to man, train, and equip for mission readiness, administration, and management of those forces under the command and control of U.S. Cyber Command. The *Concept of Operations* directs the service components assigned to U.S. Cyber Command to develop capabilities in support of operational requirements from U.S. Cyber Command, and also to provide shared situational awareness of their portions of DOD networks. Further, the *Concept of Operations* identifies and delegates areas of authority and responsibility throughout the U.S. Cyber Command organizational structure. Accompanying annexes are expected to provide greater detail about the command's plans to conduct cyberspace operations. Service component officials said their components have seen drafts of the annexes and are providing U.S. Cyber Command with input for their development, but the annexes had not been issued as of March 2011.

The *Concept of Operations* is a U.S. Cyber Command document, but DOD guidance is needed as well, since the Joint Staff is responsible for promulgating Joint Chiefs of Staff publications to provide military

[15] Joint Pub. 5-0 (Dec. 26, 2006).

guidance for the joint activities of the armed forces. Accordingly, the Joint Staff has released Joint Test Publication 3-12, its guidance for cyberspace operations that, if finalized, could provide additional guidelines for the military services and joint force commanders and supporting and supported commanders. This document has been under development since September 2009, but is still in draft. According to officials with the Joint Staff and the Office of the Under Secretary of Defense (Policy), this publication will be revised again in the spring of 2011 and may not be finalized and approved for some time after that. We previously reported on the need for DOD to update its joint doctrine that discussed cyber-related issues and definitions, in part because of the challenges that the absence of such doctrine created for the military services and the combatant commands.[16] We recommended that DOD establish a time frame for (1) deciding whether or not to proceed with a dedicated joint doctrine publication on cyberspace operations, and (2) updating the existing body of joint doctrine to include complete cyberspace-related definitions. DOD concurred with our recommendations, and the development of Joint Test Publication 3-12 represents another positive step toward providing direction to the military services, but as it is still in draft form and it could be further revised, we could not determine whether it will provide comprehensive guidance to the service component commands.

As part of their responsibility for organizing, training, and equipping cyber forces to support U.S. Cyber Command's missions, the military services are taking a total force approach—including active duty and reserve military personnel, government civilians, and civilian contractors—to staffing cyberspace operations. According to service officials, in traditional support areas such as information assurance and information technology, the services have been using civilians, as well as military personnel, because these activities take place within DOD's own networks. At the time of our review, three of the services said they may only use active duty and reserve military personnel to conduct offensive cyberspace operations, which constitutes a small percentage of cyberspace operations. However, service officials expressed concern that if offensive cyberspace operations require greater personnel resources, competing demands from other mission areas may make it difficult for the services to provide additional military personnel in support of U.S. Cyber Command's activities. These concerns may be founded particularly in light of the Secretary of Defense's plan to reduce the military end strength of

[16] GAO classified report from May 2010 on challenges to DOD's cyber efforts.

the Army and Marine Corps by 2015 and to reduce Navy personnel on shore. Additionally, officials at Air Force headquarters noted that there are some reductions in military force under way in the Air Force, including in the communications field, and that there may be some civilian reductions in the future as well. Officials with the Navy's cyber component command noted that they are expected to increase the number of cyber personnel without increasing Navy end strength, as the Navy will take personnel from other areas and move them to cyber specialties.

DOD Instruction 1100.22, *Policy and Procedures for Determining Workforce Mix* (April 12, 2010), provides guidance to the military services regarding the appropriate mix of personnel (military and DOD civilian) and private sector support for DOD activities. Specifically, it provides personnel mix criteria and guidance for risk assessments to be used to identify and justify activities that are inherently governmental or commercial. However, DOD and service officials told us that DOD is still reviewing the appropriate roles for government civilians in the cyberspace domain and service officials indicated that DOD policy guidance was insufficient to determine precisely what civilian activities or duties are permissible or prohibited in the cyberspace domain as direct participation in hostilities. The need for clarity regarding the roles government civilians may fill within the services' new cyber components creates additional challenges for the services as they develop their cyber components in support of U.S. Cyber Command.

For example, a July 2010 memorandum from the Air Force's Judge Advocate General to DOD's General Counsel raised concerns about the insufficiency of DOD's policies to determine precisely what DOD civilian activities or duties were permissible in relation to computer network attack operations and, in the absence of clarification on these matters, recommended that Air Force leadership limit DOD civilian roles in such cyberspace operations. Air Force cyber officials told us that there is uncertainty about whether they can use government civilians for DOD cyberspace missions or if only uniformed military personnel may conduct such operations. Navy officials noted that, to date, their civilian employees have focused on cyber support issues, though this may change in the future as they work to grow their civilian cyber force into other areas of cyberspace operations. Currently, some of the services are leveraging reserve component resources and are using personnel from existing career fields, such as communications and intelligence, because of limits on the total number of military personnel in each service. As a result, without greater clarity regarding the personnel options at their disposal, the military services may have difficulty in meeting their personnel

requirements in organizing, training, equipping, and providing cyber forces if the requirements for offensive cyberspace missions and personnel increase.

Certain Specific Command and Control Relationships for Cyberspace Operations Remain Unresolved

U.S. Cyber Command's *Concept of Operations* generally describes the command and control relationships between U.S. Cyber Command and the other combatant commands; however, more detailed guidance is needed to clarify these relationships between U.S. Cyber Command and the geographic combatant commands. According to DOD guidance, command and control is the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Further, command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. The Joint Chiefs of Staff joint operational planning guidance[17] indicates that command and control relationships are to be identified in the plan. U.S. Cyber Command's *Concept of Operations* recognizes that a majority of cyber operations will originate at the theater and local levels, thereby placing them under the immediate control of the geographic combatant commanders and their components, and recognizes that nearly all cyberspace operations can simultaneously affect the global, theater, and local levels because cyberspace operations can be virtually unconstrained by geography. According to its *Concept of Operations*, when a cyberspace operation is confined to the area of responsibility of one geographic combatant command, U.S. Cyber Command will act as a supporting commander to the geographic combatant commander.[18] When the cyberspace operations impact global functions or create effects across the borders of more than one geographic combatant command's area of responsibility, the

[17] Joint Pub. 5-0 (Dec. 26, 2006).

[18] In Joint Publication 1, support relationships between combatant commanders are established by the Secretary of Defense for the planning and execution of joint operations. This ensures that the tasked combatant commander(s) receives the necessary support. A supported combatant commander requests capabilities, tasks supporting DOD components, coordinates with the appropriate federal agencies, and develops a plan to achieve the common goal. As part of the team effort, supporting combatant commanders provide the requested capabilities, as available, to assist the supported combatant commander to accomplish missions requiring additional resources.

geographic combatant commanders may support U.S. Cyber Command, as directed.

However, officials from all four of the military services told us they require further specificity regarding command and control relationships for cyberspace operations, and officials from U.S. Cyber Command agreed. Of particular concern to the services is how the support relationships between U.S. Cyber Command and the geographic combatant commands discussed above will be implemented. There are several different command and control models for establishing such support relationships, but U.S. Cyber Command's *Concept of Operations* does not identify a specific model for U.S. Cyber Command and the geographic combatant commands to follow. For example, the Joint Task Force model may be established on a geographical area or functional basis when the mission has a specific limited objective and does not require overall centralized control of logistics. The commander of a joint task force exercises operational control over assigned (and normally over attached) forces and also may exercise tactical control[19] over forces or be a supported or supporting commander. Another option, which is based on the U.S. Special Operations Command model, would have U.S. Cyber Command conduct its own operations,[20] but also give it functions similar to the military services to organize, train, equip, and provide forces to the other combatant commands.[21] Another command and control model, based on U.S. Transportation Command, would have cyber forces deployed in a geographic combatant command's area of responsibility remain assigned

[19] Tactical control is defined as command authority over assigned or attached forces or commands, or military capability or forces made available for tasking, that is limited to the detailed direction and control of movements or maneuvers within the operational area necessary to accomplish missions or tasks assigned. Tactical control is inherent in operational control. Tactical control may be delegated to and exercised at any level at or below the level of combatant command. Tactical control provides sufficient authority for controlling and directing the application of force or tactical use of combat support assets within the assigned mission or task. Joint Pub. 1-02 (Nov. 8, 2010, as amended through Dec. 31, 2010).

[20] Joint Publication 1 states that U.S. Special Operations Command may conduct selected special operations, usually in coordination with the geographic combatant commander in whose area of responsibility the special operation will be conducted, as directed by the President or Secretary of Defense.

[21] The Commander of U.S. Special Operations Command has specific authority, among other powers, to exercise authority, direction, and control over the expenditure of funds for forces assigned to the special operations command and to train assigned forces. 10 U.S.C. § 167(e)(2)(C)(i) and § 167(e)(2)(D).

to and under the control of U.S. Cyber Command, unless otherwise directed.

DOD is aware of this particular challenge, and is working toward resolving it. Officials from three of the four services told us DOD and U.S. Cyber Command are beginning to address the issue, for example, by conducting a series of cyberspace command and control exercises. According to military service officials, in January 2011, DOD conducted a tabletop exercise as part of U.S. Pacific Command's larger Terminal Fury exercise to test some cyber-related command and control models. Additionally, a U.S. Cyber Command official told us that U.S. European Command will test an alternative cyberspace operations command and control model in a tabletop exercise at the end of March 2011 and during its Austere Challenge exercise in spring 2011. Further, in September 2010, the Joint Chiefs of Staff requested that U.S. Pacific Command, in coordination with U.S. Strategic Command, develop a concept of operations and initiate an Initial Capabilities Document supporting combatant commander requirements for cyberspace operations.[22] Without a clear and specific command and control relationship model, however, the services are unclear as to how, to whom, and in what form they will be required to present forces for cyberspace operations. The military services do not know whether they will be required to present trained individuals or complete mission-capable units, and they do not know if those individuals or units will be presented to U.S. Cyber Command or to regional organizations under the control of the geographic combatant commands. Until they are provided with clearer and more specific command and control relationships, it will be difficult for the services to plan the personnel, training, and budgets needed to support emerging and future cyberspace operational needs.

In our prior work, we highlighted the command and control challenges for cyberspace operations caused by conflicting guidance and unclear responsibilities.[23] This situation continues and until DOD updates its policies and guidance to clarify command and control relationships for cyberspace operations and clearly communicates those to all DOD entities, its efforts to conduct coordinated and timely cyberspace operations could be degraded.

[22] Joint Staff, Joint Requirements Oversight Council Memo 147-10: *Cyberspace Studies and Way Ahead* (Sept. 14, 2010).

[23] GAO classified report from May 2010 on challenges to DOD's cyber efforts.

Military Services Are Pursuing Diverse Service-Specific Approaches in the Absence of Information on Long-Term Mission Requirements and Capabilities Needs

The military services are pursuing diverse service-specific approaches to establishing cyberspace capabilities because, although U.S. Cyber Command has made progress in operational planning for its missions, it has not fully defined long-term mission requirements and capabilities for the military services to fulfill. The U.S. Cyber Command *Concept of Operations* provides an overall picture of U.S. Cyber Command's organization and operational relationships. However, other levels and types of guidance will be needed to provide a greater level of detail for the services and other DOD entities regarding specific issues such as, but not limited to operations, force planning, capability needs, and mission requirements. Officials from three of the four service components told us that U.S. Cyber Command has been providing them with operational guidance on an almost daily basis that is sufficient for them to conduct their current operations, but officials from the fourth service said that the guidance received to date is not enough to enable them to formalize their long-term personnel and training requirements.

To guide the services' efforts to organize, train, and equip forces for assignment to combatant commands, DOD's guidance requires that combatant commanders provide mission requirements that the services should meet. Further, combatant commanders are to provide mission requirements and desired capabilities and identify their highest-priority needs for the services to plan toward. U.S. Cyber Command's *Concept of Operations* defines its mission to include defending DOD information networks and conducting full-spectrum military cyberspace operations when directed. It also defines three specific mission areas within this broader mission: DOD Global Information Grid operations, defensive cyberspace operations (including Dynamic Network Defense Operations), and offensive cyberspace operations. Our analysis showed that the U.S. Cyber Command *Concept of Operations* generally meets the joint guidance for such documents. However, U.S. Cyber Command has not yet developed the next level of planning guidance, which would identify mission requirements and desired capabilities to guide the services' efforts to recruit, train, and provide forces with appropriate skill sets. For example, planning guidance could be provided in the form of products of the joint operational planning processes that address specific threats or contingencies, such as operational plans or concept plans.

According to officials from the four military services, the services have not yet received formalized U.S. Cyber Command guidance regarding long-term personnel requirements and capabilities, and therefore have respectively worked to develop internal guidance based on service-specific needs and missions as well as, in some cases, anticipated U.S.

Cyber Command requirements. Consequently, the services are moving forward using disparate, service-specific approaches to operationalizing cyberspace[24] without knowing exactly what mission requirements they will be required to meet for U.S. Cyber Command. For example, Navy and Air Force officials told us that they are leveraging reserve component resources and taking personnel from existing career fields to avoid having to increase service end strength. Further, the two services are taking very different approaches to rearranging their career fields to varying degrees in order to further improve their efforts to recruit and retain cyber personnel, and they are doing this in different ways as they define new service-level personnel needs, maintain old ones, anticipate future U.S. Cyber Command personnel needs, and attempt to recruit, retain, and train for all three needs. Army, Navy, and Marine Corps officials told us that they are largely rearranging existing specialty codes in communications and cryptologic fields and giving their personnel new tasks and some new training, while the Air Force has created entirely new career specialties for cyberspace operations.

Cyber personnel training is another area in which the services are challenged by their need for mission requirements and capabilities from U.S. Cyber Command. In the absence of requirements from U.S. Cyber Command, the services have started to develop their own cyber training programs geared toward service-specific cyberspace requirements and attempts to anticipate the future needs of U.S. Cyber Command. For example, officials from all four of the services told us that they have preexisting training programs to address well-established information assurance and computer network defense training needs. For the emerging area of offensive cyberspace operations, the Navy and Marine Corps rely heavily on the Joint Cyber Analysis Course, run by the Navy as the executive agent under the National Security Agency's Cryptologic Training System. Army officials told us that the service makes some use of this National Security Agency–sponsored course, but also has service-specific training of its own. Both the Army and the Navy see their separate training courses as candidates for future joint cyber training, though no decision has been made yet in this regard. Air Force cyber officials told us that the service utilizes the Joint Cyber Analysis Course to provide personnel to fill National Security Agency positions, but also established

[24] We are using the phrase "operationalizing cyberspace" to refer to the emerging concept of conducting military operations in cyberspace, as opposed to utilizing cyberspace only as a supporting function in the more familiar domains of land, sea, air, and space.

two training courses in 2010—one for officers and one for enlisted—to meet its own cyberspace operations needs. Requirements for both courses are set by the Air Force's Air Education and Training Command and Air Force Space Command, though the Air Force has received some informal input from U.S. Cyber Command. However, U.S. Cyber Command has not specified whether it will be requesting personnel from the services according to (1) the knowledge, skills, and abilities required; (2) occupational specialties; (3) grade structures; or (4) another category. Without specific mission and capabilities requirements, the military services cannot determine the requirements based on which they are to provide and train personnel for the long term, or the capabilities they will be expected to provide to U.S. Cyber Command. Therefore, the cyber personnel and capabilities may vary from service to service. Differences between the services can be good and may be expected, but whether these differences are beneficial in the case of cyberspace operations, and whether the services will be able to meet U.S. Cyber Command's long-term mission requirements once they are established, remain unknown.

Conclusions

Establishing a new command and the service components needed to support it constitutes a large undertaking within DOD, requiring much planning and coordination. DOD and the military services have already laid the foundation and built a framework for the new U.S. Cyber Command and its service components in little more than a year, a significant achievement in an emerging domain. However, much work still needs to be done in a timely manner to mature the operational capabilities of U.S. Cyber Command and the service cyber components to a level comparable to those of their peers in the air, land, sea, and space domains. Joint test documents, broad definitions, and general outlines of roles, responsibilities, and organizational structures are an important starting point in building an effective organization, but detailed and formalized guidance is needed to clarify roles, responsibilities, command structures, and mission requirements. Until such detailed guidance is articulated, the military services will continue to move forward in planning, budgeting, recruiting, and training personnel to conduct cyberspace operations without knowing whether their efforts will meet U.S. Cyber Command's mission needs.

Recommendations for Executive Action

We recommend that the Secretary of Defense take the following three actions regarding U.S. Cyber Command and its service components' cyberspace operations.

To assist the military services in fulfilling their responsibilities to organize, train, and equip cyber forces, we recommend that the Secretary of Defense set a timeline and direct the:

- Under Secretary of Defense for Policy and the Under Secretary of Defense for Personnel and Readiness, in consultation with the DOD Office of General Counsel, to develop and publish detailed policies and guidance pertaining to categories of personnel that can conduct the various forms of cyberspace operations;
- Chairman of the Joint Chiefs of Staff to develop and publish authoritative and specific guidance regarding the supporting and supported command and control relationships between U.S. Cyber Command and the geographic combatant commands for cyberspace operations; and
- Commander, U.S. Strategic Command, in conjunction with U.S. Cyber Command, to develop and publish authoritative and specific guidance regarding the mission requirements and capabilities, including skill sets, that the services should meet to provide long-term operational support to U.S. Cyber Command.

Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD agreed with all of our recommendations and stated that they are taking actions to address these issues internally. DOD also stated that each of the actions we recommended is important or highly desirable to accomplish. However, DOD did not provide the timelines expected for completing these actions. Such timelines would assist the military services in their planning processes by letting them know when they can expect much-needed guidance pertaining to the categories of personnel that can conduct cyberspace operations; clarified roles and responsibilities for command and control relationships between U.S. Cyber Command and the geographic combatant commands; and mission requirements from DOD. DOD's comments appear in their entirety in appendix II. DOD also provided technical comments, which we have incorporated as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the appropriate congressional committees; the Secretary of Defense; the Secretary of the Army; the Secretary of the Navy; the Secretary of the Air Force; the Commandant of the Marine Corps; the Commander of U.S. Strategic Command; and the Commander of U.S. Cyber Command. In

addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions about this report, please contact me at (202) 512-5431 or at dagostinod@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors to this report are listed in appendix III.

Davi M. D'Agostino
Director
Defense Capabilities and Management

List of Requesters

The Honorable Adam Smith
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable W. "Mac" Thornberry
Chairman
The Honorable Jim Langevin
Ranking Member
Subcommittee on Emerging Threats and Capabilities
Committee on Armed Services
House of Representatives

Appendix I: Scope and Methodology

Objectives

This report addresses the extent to which the Department of Defense (DOD) and U.S. Cyber Command have identified for the military services (1) roles and responsibilities including categories of personnel that can conduct various cyberspace operations; (2) command and control relationships, to include the geographic combatant commands; and (3) mission requirements and capabilities in support of U.S. Cyber Command to enable them to organize, train, and equip for cyberspace operations.

Scope and Methodology

To address our objectives, we focused our work on the four active duty DOD military services—Army, Navy, Marine Corps, and Air Force. We focused our review on the efforts of the four military services to organize cyber service component commands and provide appropriately trained and equipped personnel in support of both their own and U.S. Cyber Command's mission needs. This includes activities in the areas of computer network defense, exploitation, and computer network attack. We reviewed a variety of unclassified and classified documents related to the organization and challenges the department faces in addressing cyberspace operations.

To evaluate the military services' cyberspace efforts, we reviewed classified and unclassified documents and interviewed officials from a range of DOD and military service organizations involved either directly in cyberspace operations or in the services' role of organizing, training, and equipping forces for cyberspace operations. Table 2 lists the DOD offices we contacted.

Table 2: DOD Entities Visited or Contacted during Our Review

DOD organization	Entity visited or contacted
Department of Defense	• Office of General Counsel, Pentagon, Washington, DC • Office of the Chief of Information Operations, Pentagon, Washington, DC
Office of the Secretary of Defense	• Office of the Under Secretary of Defense for Policy, Pentagon, Washington, DC
Joint Staff	• J39, Operations, Pentagon, Washington, DC • J5, Strategic Plans and Policy, Pentagon, Washington, DC
U.S. Strategic Command	• J882, Capability and Resource Integration, Cyber Defense Capabilities, Offutt Air Force Base, Omaha, NE
U.S. Cyber Command	• Fort Meade, MD

DOD organization	Entity visited or contacted
U.S. Army	• Army Headquarters G3, Cyber Directorate, Arlington, VA
	• Army Cyber Command/2nd Army, Fort Belvoir, VA
	• Army Training and Doctrine Command, Fort Monroe, VA
	• Army Combined Arms Center, Fort Leavenworth, KS
	• Army Signal Center, Fort Gordon, GA
	• Army Intelligence Center, Fort Huachuca, AZ
U.S. Navy	• Department of the Navy, Office of the Chief of Information Operations, Pentagon, Washington, DC
	• Office of the Chief of Naval Operations, Pentagon, Washington, DC
	• Fleet Cyber Command/10th Fleet, Fort Meade, MD
	• Navy Center for Information Dominance, Corry Station, FL
U.S. Marine Corps	• Headquarters Marine Corps, Information Assurance Division, Quantico, VA
	• Marine Forces Cyber Command, Columbia, MD
	• Marine Corps Training and Education Command, Quantico, VA
	• Marine Corps Training Command, Quantico, VA
	• Marine Corps Communication Electronics Schools, Twentynine Palms, CA
U.S. Air Force	• Air Force Headquarters, Directorate for Cyber and Information Operations, Pentagon, Washington, DC
	• Air Force Space Command, Peterson Air Force Base, CO
	• Air Education and Training Command, Randolph Air Force Base, TX
	• 24th Air Force/Air Force Cyber Command, Lackland Air Force Base, TX
	• 333rd Training Squadron, Keesler Air Force Base, MS
	• 39th Information Operations Squadron, Hurlburt Field, FL
National Security Agency	• Associate Directorate for Education and Training, Fort Meade, MD

Source: GAO data.

To assess the extent to which roles and responsibilities for the military services had been identified for cyberspace operations, we reviewed DOD doctrine and policy and interviewed relevant officials from DOD, U.S. Cyber Command, and the four military services. Specifically, we reviewed Joint Publication 1, *Doctrine for the Armed Forces of the United States* (May 2, 2007, incorporating Change 1, March 20, 2009); DOD Directive 5100.01, *Functions of the Department of Defense and Its Major Components* (December 21, 2010); and joint guidance related to the Joint Operation Planning and Execution System[1] to identify the criteria,

[1] Joint Chiefs of Staff, Joint Publication 5-0: *Joint Operational Planning* (Dec. 26, 2006); Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3122.01A: *Joint Operation Planning and Execution System Volume I, Planning Policies and Procedures* (Sept. 29, 2006, current as of Oct. 11, 2008); and CJCSM 3122.03C: *Joint Operation Planning and Execution System Volume II, Planning Formats and Guidance* (Aug. 17, 2007).

definitions, and other guidance that DOD and U.S. Cyber Command should be following as they identify the appropriate roles and responsibilities for the military services and other organizations that support DOD cyberspace operations. We then compared these joint documents to the guidance and information provided to us by officials at the DOD General Counsel's Office, U.S. Cyber Command, and its supporting service commands to assess whether any gaps existed. Specifically, we reviewed U.S. Cyber Command's *Concept of Operations* (September 21, 2010) and DOD Instruction 1100.22, *Policy and Procedures for Determining Workforce Mix* (April 12, 2010).

To assess the extent to which DOD had addressed command and control issues for cyberspace operations, we reviewed DOD directives, doctrine, and policy and interviewed relevant officials from DOD, U.S. Cyber Command, and the four military services. Specifically, we reviewed DOD Directive 5100.01; Joint Publication 1; Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* (November 8, 2010, as amended through December 31, 2010); Joint Publication 5-0; and the 2008 *Unified Command Plan* to identify criteria for delineating "supported" and "supporting" command and control relationships between combatant commands and the military services. We compared these documents to guidance and information provided to us by officials at U.S. Cyber Command—specifically the *Concept of Operations* (September 21, 2010)—to determine to what extent U.S. Cyber Command has defined these relationships. We also reviewed Joint Publication 1, Joint Publication 1-02, and the 2008 *Unified Command Plan* and interviewed officials from the military services to identify possible command and control models that U.S. Cyber Command could use in developing its relationships with the geographic combatant commands and the military services.

To assess mission requirements and capabilities issues, we reviewed DOD doctrine and interviewed relevant officials from DOD, U.S. Cyber Command, and the four military services. Specifically, we reviewed joint guidance related to the Joint Operation Planning and Execution System[2] to determine the criteria that joint commands are to follow when developing doctrine and guidance, specifically in regard to mission requirements and capability needs at various stages of operational capability. We compared

[2] Joint Pub. 5-0 (Dec. 26, 2006); CJCSM 3122.01A (Sept. 29, 2006, current as of Oct. 11, 2008); and CJCSM 3122.03C (Aug. 17, 2007).

the Joint Operation Planning and Execution System criteria to the guidance and information provided to us by officials at U.S. Cyber Command—specifically the *Concept of Operations* (September 21, 2010)—and its supporting service commands to assess whether any gaps existed.

We conducted this performance audit from May 2010 to May 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Comments from the Department of Defense

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
2900 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-2900

GLOBAL
STRATEGIC AFFAIRS

April 29, 2011

Ms. Davi M. D'Agostino
Director, Defense Capabilities and Management
U. S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. D'Agostino:

Thank you for the opportunity to comment on the GAO Draft Report, GAO-11-421 "DEFENSE DEPARTMENT CYBER EFFORTS: More Detailed Guidance Needed to Ensure Military Services Develop Appropriate Cyberspace Capabilities," dated March 29, 2011" (GAO Code 351490).

Enclosed are the Department's response to the recommendations and the Department Technical Comments to this draft report.

Your report will help in the education of our U.S. Government seniors, as the Department moves forward in this domain of cyberspace.

If you have further questions, please do not hesitate to contact myself or my point of contact, Mr. Michael Cooksey at (571) 256-7809, Michael.Cooksey@osd.mil

Sincerely,

Robert J. Butler
Deputy Assistant Secretary of Defense,
Cyber Policy

Enclosure:
As stated

GAO DRAFT REPORT DATED MARCH 29, 2011
GAO-11-421 (GAO CODE 351490)

"DEFENSE DEPARTMENT CYBER EFFORTS: MORE DETAILED GUIDANCE NEEDED TO ENSURE MILITARY SERVICES DEVELOP APPROPRIATE CYBERSPACE CAPABILITIES"

DEPARTMENT OF DEFENSE COMMENTS TO THE GAO RECOMMENDATIONS

RECOMMENDATION 1: The GAO recommends that the Secretary of Defense set a timeline and direct the Undersecretary for Policy and the Undersecretary of Defense for Personnel and Readiness, in consultation with the DoD Office of General Counsel, to develop and publish detailed policies and guidance pertaining to categories of personnel who can conduct the various forms of cyberspace operations.

DoD RESPONSE: The Department of Defense concurs with comment to the GAO recommendation. The Department agrees the development and publication of policies and guidance pertaining to categories of personnel who can conduct the various forms of cyberspace operations is important and the Department is working internally to look at these issues.

RECOMMENDATION 2: The GAO recommends that the Secretary of Defense set a timeline and direct the Chairman of the Joint Chiefs of Staff to develop and publish authoritative and specific guidance regarding the supporting and supported command and control relationships between U.S. Cyber Command and the geographical combatant commands for cyberspace operations.

DoD RESPONSE: The Department of Defense concurs with comment to the GAO recommendation. The Department agrees that the development and publication of an authoritative and specific guidance regarding the supporting and supported command and control relationships between U.S. Cyber Command and the geographical combatant commands for cyberspace operations is important and that the Department is working internally to look at these issues.

RECOMMENDATION 3: The GAO recommends that the Secretary of Defense set a timeline and direct the Commander, U.S. Strategic Command, in conjunction with U.S. Cyber Command, to develop and publish authoritative and specific guidance regarding the mission requirements and capabilities, including skill sets that the services should meet to provide long-term operational support to the U.S. Cyber Command.

DoD RESPONSE: The Department of Defense concurs with comment to the GAO recommendation. The Department agrees that the development and publication of authoritative and specific guidance regarding the mission requirements and capabilities, including skill sets that the services provide to U.S. Cyber Command is highly desirable and the Department is working internally to look at these issues.

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Davi M. D'Agostino, (202) 512-5431 or dagostinod@gao.gov

Staff Acknowledgments

In addition to the contact named above, Penney Harwell Caramia, Assistant Director; Neil Feldman; Katherine Forsyth; Bridget Grimes; Joseph Kirschbaum; Katherine Lenane; Gregory Marchand; Bethann Ritter; Michael Silver; Amie Steele; and Cheryl Weissman made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548