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.