July 2011

DEFENSE DEPARTMENT CYBER EFFORTS

DOD Faces Challenges In Its Cyber Activities

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-11-75, a report to congressional requesters

Why GAO Did This Study

According to the U.S. Strategic Command, the Department of Defense (DOD) is in the midst of a global cyberspace crisis as foreign nation states and other actors, such as hackers, criminals, terrorists, and activists exploit DOD and other U.S. government computer networks to further a variety of national, ideological, and personal objectives. This report identifies (1) how DOD is organized to address cybersecurity threats; and assesses the extent to which DOD has (2) developed joint doctrine that addresses cyberspace operations; (3) assigned command and control responsibilities; and (4) identified and taken actions to mitigate any key capability gaps involving cyberspace operations. It is an unclassified version of a previously issued classified report. GAO analyzed policies, doctrine, lessons learned, and studies from throughout DOD, commands, and the services involved with DOD's computer network operations and interviewed officials from a wide range of DOD organizations.

What GAO Recommends

GAO recommends that DOD (1) establish a timeframe for deciding on whether to complete a separate joint cyberspace publication and for updating the existing body of joint publications, (2) clarify command and control relationships regarding cyberspace operations and establish a timeframe for issuing the clarified guidance, and (3) more fully assess cyber-specific capability gaps, and (4) develop a plan and funding strategy to address them. DOD agreed with the recommendations.

View GAO-11-75 or key components. For more information, contact Davi M. D'Agostino at (202) 512-5431 or dagostinod@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

DOD's organization to address cybersecurity threats is decentralized and spread across various offices, commands, military services, and military agencies. DOD cybersecurity roles and responsibilities are vast and include developing joint policy and guidance and operational functions to protect and defend its computer networks. DOD is taking proactive measures to better address cybersecurity threats, such as developing new organizational structures, led by the establishment of the U.S. Cyber Command, to facilitate the integration of cyberspace operations. However, it is too early to tell if these changes will help DOD better address cybersecurity threats.

Several joint doctrine publications address aspects of cyberspace operations, but DOD officials acknowledge that the discussions are insufficient; and no single joint publication completely addresses cyberspace operations. While at least 16 DOD joint publications discuss cyberspace-related topics and 8 mention "cyberspace operations," none contained a sufficient discussion of cyberspace operations. DOD recognizes the need to develop and update cyber-related joint doctrine and is currently debating the merits of developing a single cyberspace operations joint doctrine publication in addition to updating all existing doctrine. However, there is no timetable for completing the decision-making process or for updates to existing doctrine.

DOD has assigned authorities and responsibilities for implementing cyberspace operations among combatant commands, military services, and defense agencies; however, the supporting relationships necessary to achieve command and control of cyberspace operations remain unclear. In response to a major computer infection, U.S. Strategic Command identified confusion regarding command and control authorities and chains of command because the exploited network fell under the purview of both its own command and a geographic combatant command. Without complete and clearly articulated guidance on command and control responsibilities that is well communicated and practiced with key stakeholders, DOD will have difficulty in achieving command and control of its cyber forces globally and in building unity of effort for carrying out cyberspace operations.

DOD has identified some cyberspace capability gaps, but it has not completed a comprehensive, departmentwide assessment of needed resources, capability gaps, and an implementation plan to address any gaps. For example, U.S. Strategic Command has identified that DOD's cyber workforce is undersized and unprepared to meet the current threat, which is projected to increase significantly over time. While the department's review of some cyberspace capability gaps on cyberspace operations is a step in the right direction, it remains unclear whether these gaps will be addressed since DOD has not conducted a more comprehensive departmentwide assessment of cyber-related capability gaps or established an implementation plan or funding strategy to resolve any gaps that may be identified.