Evolution of US Strategy and Cyberspace

Proficiency Code: A

Under the authorities of the Secretary of Defense (SecDef), the Department of Defense (DOD) uses cyberspace capabilities to shape cyberspace and provide integrated offensive and defensive options for the defense of the nation. The United States Cyber Command (USCYBERCOM) coordinates with CCMDs, the JS, and the Office of the Secretary of Defense (OSD); liaises with other USG departments and agencies; and, in conjunction with the following:

- Department of Homeland Security (DHS)
- Department of Defense Cyber Crime Centers (DC3)
- Defense Security Service
- Defense Industrial Base (DIB)

Similarly, as directed, DOD deploys necessary resources to support efforts of other US Government (USG) departments, agencies, and allies. *The National Military Strategy* and *The Department of Defense Cyber Strategy* provide high-level requirements for national defense in cyberspace and DOD's role in defending DOD and larger US national security interests through Cyberspace Operations (CO).

DOD's Roles and Initiatives in Cyberspace. DOD's roles in cyberspace are, for the most part, the same as they are for the physical domains. As a part of its role to defend the nation from threats in cyberspace, DOD prepares to support DHS and the Department of Justice (DOJ), the USG leads for incident response activities during a national cybersecurity incident of significant consequences. To fulfill this mission, DOD conducts military operations to defend DOD elements of Critical Infrastructure and Key Resources (CI/KR) and, when ordered, defend CI/KR related to vital US interests. DOD's national defense missions, when authorized by Presidential orders or standing authorities, take primacy over the standing missions of other departments or agencies. *The Department of Defense Cyber Strategy* establishes strategic initiatives that offer a roadmap for DOD to operate effectively in cyberspace, defend national interests, and achieve national security objectives.

Commanders integrate CO into their operations at all levels. Their plans should address how to effectively integrate cyberspace capabilities, counter adversaries' use of cyberspace, identify and secure mission-critical cyberspace, access key terrain in cyberspace, operate in a degraded environment, efficiently use limited cyberspace assets, and pair operational requirements with cyberspace capabilities. The commander provides initial planning guidance, which may specify time constraints, outline initial coordination requirements, authorize the movement of forces within the commander's authority, and direct other actions as necessary. Supporting CO plans and concepts describe the role and scope of CO in the commander's effort and address how CO support the execution of the supported plan. If requested by a commander, USCYBERCOM provides assistance in integrating cyberspace forces and capabilities into the commander's plans and orders.

Sources: JP 3-12