SSI
STRATEGIC STUDIES INSTITUTE

Executive Summary

Strategic Studies Institute and U.S. Army War College Press

UNITED STATES
ARMY WAR COLLEGE
PRESS
Carlisle Barracks, PA
STRENGTH and WISDOM

IMPLICATIONS OF SERVICE CYBERSPACE COMPONENT COMMANDS FOR ARMY CYBERSPACE OPERATIONS

Jeffrey L. Caton

A fundamental tenet of the 2015 *DoD Cyber Strategy* is to achieve and maintain cybersecurity by a joint team effort across the whole-of-government. Some of the key Department of Defense (DoD) members of this cyberspace team are the service component cyber commands that report to U.S. Cyber Command (USCYBERCOM). U.S. Army Cyber Command (ARCYBER) conducts cyberspace-related missions of which some are common to the other service components and others are unique. To perform efficiently and effectively as part of the joint Cyber Mission Force (CMF), it is important for Army leaders and policymakers to understand the interfaces and boundaries among the service cyberspace components. Such knowledge can help to avoid unnecessary duplication as well as provide venues for sharing lessons learned and best practices.

The emerging DoD CMF includes forces from all military services that may reflect artifacts in their organization, training, and operation that are influenced by service cultures. Such diversity offers challenges and opportunities for senior leaders and policymakers entrusted with creating a joint force that can operate professionally in and through cyberspace.

This monograph examines how the Army may benefit by adopting processes and practices from other service cyberspace forces to the operations of ARCYBER. It focuses on the central question: “What is the context in which different military services approach cyberspace component operations internally as well as with the DoD?” To address this question, the study is divided into four major sections. The first section provides a background of the mission and structure of USCYBERCOM and the tenets of current joint cyberspace operations doctrine. Next, the monograph explores the mission, organization, training, and equipping of each of the four service cyberspace components as well as the Coast Guard contributions. The third section analyzes how the service components support the USCYBERCOM mission as well as common trends and service culture influences among their operations. Finally, the author provides recommendations for DoD and Army leaders to consider for the enhancement of joint and service cyberspace operations.

The material presented herein is limited to unclassified and open source information available before September 2017, thus any classified discussion must occur within other venues. Also, the discussion regarding service cyberspace components will not be comprehensive due to classification and space requirements; instead, the monograph uses representative examples or illustrative vignettes to guide the discourse. The monograph includes recommendations related to cyber training ranges, cyber professional development, doctrine, and integration with operations in traditional domains.

*****

More information about the programs of the Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press may be found on the Institute’s homepage at *http://ssi.armywarcollege.edu/.*

*****

This Publication

SSI Website

USAWC Website