This product is part of the RAND Corporation documented briefing series. RAND documented briefings are based on research briefed to a client, sponsor, or targeted audience and provide additional information on a specific topic. Although documented briefings have been peer reviewed, they are not expected to be comprehensive and may present preliminary findings.

DOCUMENTED
BRIEFING

Human Capital Management for the USAF Cyber Force

Lynn M. Scott, Raymond E. Conley, Richard Mesic, Edward O'Connell, Darren D. Medlin

Prepared for the United States Air Force

PROJECT AIR FORCE

The research described in this report was sponsored by the United States Air Force under Contract FA7014-06-C-0001. Further information may be obtained from the Strategic Planning Division, Directorate of Plans, Hq USAF.

Library of Congress Cataloging-in-Publication Data

Human capital management for the USAF cyber force / Lynn M. Scott ... [et al.].
p. cm.
Includes bibliographical references.
ISBN 978-0-8330-4749-6 (p : alk. paper)
1. United States. Air Force Space Command—Planning. 2. United States—Personnel management.
3. Information warfare—United States. 4. Cyberspace—Security measures. I. Scott, Lynn M.

UG1523.H86 2010
358.4'161—dc22

2009050698

The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

RAND® is a registered trademark.

Published 2010 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

Summary

The Air Force announced its intent to create a formal organization dedicated to cyberspace capabilities in September 2006. The organization's purpose is to provide combat-ready forces trained and equipped to conduct sustained offensive and defensive global operations in and through cyberspace that are fully integrated with air and space operations. RAND was asked to identify and analyze the human capital management issues associated with this transformation. The research addressed four questions relevant to creating a sustainable cyber force:

1. What kinds of cyber capabilities will the cyber force be required to produce?
2. How will the cyber force be distributed in Air Force organizations?
3. What skills should the cyber force possess and how should they be distributed by military grade, civilian, contractor, and functional domains?
4. What kind of military specialty classification structure will lead to a viable, sustainable cyber force?

The Air Force's cyberspace concept of operations and organizational structure was still evolving when this research was being conducted. As a consequence, this study was designed to be strategically oriented and comprehensive for broad application depending on the courses of action the Air Force eventually selects. We sought data and information to answer the research questions from numerous sources. They included current doctrine, strategic planning documents, Air Force manpower databases, and interviews with career field managers and senior leaders and staff responsible for current cyber and information operations capabilities.

The Air Force is at the initial stages of developing fully integrated cyber capabilities that include cyber attack, cyber defense, and cyber exploitation. Its goal for kinetic and nonkinetic strike capability will depend on how successfully it can integrate cyber capabilities with existing information operations and air or space capabilities and specify the effects that will be produced from that integration. Additionally, the Air Force needs to initiate substantive planning for integrating its envisioned capabilities with other military and government agencies that provide similar or complementary capabilities. The Air Force's specification of how it will integrate cyber capabilities functionally and organizationally to produce capabilities and effects will ultimately define how it will operate in cyberspace. That refined definition will guide the requirements for cyber human capital in skill and number.

The Air Force has to meet the challenge to organize, train, and equip its cyber force to successfully prevail in any number of warfare scenarios. Moreover, it must develop its force to effectively confront the increasing use of cyber-based tools and techniques in irregular warfare and counterinsurgencies—forms of warfare most closely associated with the war on terrorism.

Overall, the level and number of skill sets required to effectively perform future cyber missions will grow in response to the increasing sophistication in the skill sets of potential adversaries.

However, the Air Force faces an immediate challenge in managing human capital. There is a limited supply of personnel with the requisite skills to comprise a cyber force that can deliver the capabilities envisioned by the Air Force. The cyber organizations analyzed in this research had two types of positions: those with requirements for skills from traditional specialties (e.g., communications-computer, intelligence, developmental engineering, electronic warfare operations) and those that require an augmentation of traditional specialty skills with skills and knowledge associated with specific capabilities: computer network attack, computer network defense, and computer network exploitation. These positions have "cyber-hybrid" requirements and they exist for officers, enlisted personnel, and civilians (see pp. 18–22).

Most airmen are developed for these cyber-hybrid jobs through organizationally specific on-the-job training programs. This training results in just-in-time cyber skills for just enough cyber personnel. Because we estimate that about 2,600 cyber-hybrid jobs exist throughout the Air Force, we believe that a decentralized, organizationally specific development approach is not enough to build a sustainable cyber workforce. Consequently, more-aggressive human capital management strategies are needed to increase the pools of highly skilled talent for computer network defense, computer network attack, and computer network exploitation. We conclude that the most immediate policy action the Air Force can take to build cumulative cyber experience is to customize accession-level Air Force Specialty Codes (AFSCs), lateral AFSCs, and AFSC suffixes for the major Air Force specialties that contribute to cyber missions. (see p. 27).

We also speculate about the kinds of skills the cyber force will need in the future, based on a scenario in which Air Force cyber capabilities are fully integrated with air and space capabilities in about 2020. The scenario also assumes that some Air Force cyber capabilities may be applied during peacetime, in conjunction with other government agencies, as well as in different forms of warfare. We conclude that Air Force cyber personnel will need additional technical, legal, organizational, and operational skills (see pp. 32–33).

We recommend several concrete steps that the Air Force can take to manage its cyber human capital (see pp. 36–37):

1. Establish a more comprehensive concept of operations (CONOPS) that addresses the functional, organizational, and operational integration needed to create highly valued capabilities and how the Air Force will operate in and through cyberspace throughout the peace-war-reconstitution spectrum of activities. The scope of the cyber domain is large, encompassing technical, functional, and strategic dimensions of national security. The revised CONOPS should align Air Force planning with the functional, organizational, and operational complexities inherent in mitigating cyber vulnerabilities and cyber threats and conducting cyber warfare.
2. Use the revised CONOPS as a basis for stakeholders to specify total-force human capital requirements (i.e., for active duty and reserve components, Air Force civilians, and contractors). More-comprehensive specifications of cyber operations should add precision to the Air Force's specification of the cyber-based skills needed in the force, its classification structure for cyber skills management, and its identification of the best combination of sources within the total force for these skills.

3. Establish a lateral officer AFSC as a method to manage cyber skills, particularly for policy, doctrine, planning, and programming jobs that will require people steeped in cyber; use AFSC suffixes to manage cyber skills within other officer specialties. Classification policies can greatly contribute to strategies for building mission-critical skill sets at technical, operational, and leadership levels. Because of its traditional use to broaden and enhance the utilization of personnel, a lateral-entry AFSC would contribute to quickly building leaders in the cyber domain.
4. Continue efforts to retool the enlisted communications-computer specialty into an accession-entry cyber specialty, and use suffixes and special experience identifiers to manage cyber skills in other specialties, such as intelligence. These skill sets within enlisted communications-computer specialties are highly congruent with cyber skill sets in network operations, and this congruency supports the use of an accession-entry specialty. For specialties such as intelligence, which have less congruence with cyber skills, the use of suffixes and special experience identifiers will be sufficient for personnel identification and management.
5. Continuously assess the cyber force's sustainability. Cyber capabilities, vulnerabilities, and threats are evolving rapidly. Furthermore, skilled cyber personnel may be attracted to career opportunities in the civilian sector. To keep pace with these challenges, the Air Force should assess cyber skill requirements routinely to ascertain whether current policies and practices will sustain the force.