Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **2010**	2. REPORT TYPE	3. DATES COVERED **00-00-2010 to 00-00-2010**

4. TITLE AND SUBTITLE
Human Capital Management for the USAF Cyber Force

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Rand Corporation,1776 Main Street,PO Box 2138,Santa Monica,CA,90407-2138

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**57**	

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

Approved for public release; distribution unlimited

RAND 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.

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

Preface

In late 2006, the Air Force announced that cyberspace would constitute a new mission domain for the service, along with air and space domains. Since that announcement, the Air Force has developed an organizational construct in which Air Force Space Command will oversee the preparation of combat-ready forces to conduct sustained offensive and defensive global operations in and through cyberspace and will present cyberspace forces to combatant commanders through a component numbered Air Force. A vital component of the Air Force's envisioned cyber capabilities is the human capital that will make up the cyber force. The human capital management and development policies will have far-reaching implications for the kind of skilled cyber force the Air Force has today and in the future.

The research described in this report was sponsored by three Headquarters United States Air Force (HAF) offices: Warfighting Integration (SAF/XC), Cyber Operations (AF/A3O-C), and the Development Directorate within Manpower and Personnel (AF/A1D). Its objective was to identify and analyze the human capital management issues associated with the creation and management of a cyber force. The work was performed as part of a fiscal year 2007 study, "USAF Specialty Code Restructuring," and conducted within the Manpower, Personnel, and Training Program of RAND Project AIR FORCE.

This documented briefing contains slides and text that describe the background, methodology, and findings of the study. It concludes with recommendations about how the Air Force should pursue the creation and management of a highly skilled cyber force. The documented briefing should be of interest to those involved in human capital management policy and the design of workforce development strategies for computer network operations capabilities in the armed forces and many government agencies.

RAND Project AIR FORCE

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, is the U.S. Air Force's federally funded research and development center for studies and analyses. PAF provides the Air Force with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future aerospace forces. Research is conducted in four programs: Force Modernization and Employment; Manpower, Personnel, and Training; Resource Management; and Strategy and Doctrine.

Additional information about PAF is available on our Web site:
http://www.rand.org/paf/

Contents

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 non-kinetic 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 spe¬cialties (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 com¬puter network defense, computer network attack, and computer network exploitation. We con¬clude 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 capa¬bilities 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 differ¬ent forms of warfare. We conclude that Air Force cyber personnel will need additional techni¬cal, 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, organiza¬tional, 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 preci¬sion 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. 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 preci¬sion 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. 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.

Acknowledgments

The RAND project team thanks the many individuals whose effort made this research possible. Lt Gen William T. Lord (formerly SAF/XCI and later Commander, Air Force Cyber Command (Provisional), Joseph M. McDade Jr. (formerly AF/A1D), and Col Michael Butler (formerly AF/A3O-C) sponsored the research.

Several Air Force senior leaders made time to participate in the study. Their candid and insightful assessments about the vision to create the then-planned Air Force Cyber Command and the many challenges that needed to be overcome to realize the vision helped refine the focus of the study and our analysis approach. We especially appreciate the diligent efforts of their administrative staff who found the typically scarce time windows for our interviews.

We acknowledge continuous support from staff members in the Air Force and Joint organizations we relied on to gain in-depth knowledge about current cyber and information operations capabilities and Air Force Cyber Command development plans. In particular, we thank Communications-Computer Career Field Managers CMSgt Bruce Collett, CMSgt Brian Hale, and CMSgt Jeff Nelson; Intelligence Career Field Managers CMSgt Frank Pazdernick and SMSgt Keith Owen; SMSgt Corina Benetiz, 67th NWW/XP; Maj Diane Clemens, AF/A3O-CP; Maj Tim Franz, AFCYBER (P); Mike Kretzer, AFIOC; and Maj Brett Scarborough, AF/A3O-CP.

Finally, numerous RAND colleagues made valuable contributions throughout this research effort. Gary Massey created the customized manpower databases that we used to identify the human capital footprint in Air Force cyber organizations. Melanie Sisson assisted during interviews with subject matter experts, gathered data on Air Force and information operations capabilities, and conducted an analysis to identify possible trajectories of an Air Force cyberspace organization's long-term growth. Col Darren Medlin, a 2006–2007 RAND Air Force Fellow, contributed to the formulation of a future cyber scenario. William Komiss, a 2007 RAND summer associate from Stanford University, designed and conducted sustainability analyses to identify possible problems with cyber force structure. Karin Suede provided critical administrative support and coordination for our geographically dispersed team members, who often found themselves in different corners of the world during the project.

Abbreviations

ACC	Air Combat Command
ACOMS	Air Communications Squadron
AETC	Air Education and Training Command
AF	Air Force
AF/A1	Air Force Deputy Chief of Staff for Manpower and Personnel
AF/A1D	Air Force Director of Personnel, Development
AF/A1P	Air Force Director of Personnel Policy
AF/A3/5	Air Force Director of Operations and Plans
AF/A3O-C	Air Force Director for Cyber Operations
AFCA	Air Force Communications Agency
AFCYBER (P)	Air Force Cyber Command (Provisional)
AFIOC	Air Force Information Operations Center
AFNOC	Air Force Network Operations Center
AFR	Air Force Reserve
AFS	Air Force Specialty
AFSC	Air Force Specialty Code
AFSOC	Air Force Special Operations Command
AFSPC	Air Force Space Command
AIA	Air Intelligence Agency
AIS	Air Intelligence Squadron
ANG	Air National Guard
AOC	Air Operations Center
C2	command and control
C2ISR	command, control, intelligence, surveillance, and reconnaissance
C4	command, control, communications, and computers
CBT	combat
CIA	Central Intelligence Agency
CNA	computer network attack

CNE	computer network exploitation
Comm	communication
CONOPS	concept of operations
CSAF	Chief of Staff of the Air Force
CW	cyber warfare
DAF	Department of the Air Force
Det	detachment
DIA	Defense Intelligence Agency
Div	division
Elec	electronic
Enl	enlisted
EW	electronic warfare
EWF	electronic warfare flight
EWO	electronic warfare officer
EWS	electronic warfare squadron
FTU	field training unit
GP	group
HAF	Headquarters United States Air Force
HR	human resource
IADS	Integrated Air Defense Systems
Infr Sys	Infrastructure Systems
Intel	intelligence
IO	information operations
IOG	Information Operations Group
IOS	Information Operations Squadron
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
IWF	Information Warfare Flight
JCS	Joint Chiefs of Staff
JFACC	Joint Forces Air Component Commander
JIOWC	Joint Information Operations Warfare Command
KSAs	knowledge, skills, and abilities
MAJCOM	major command
MILDEC	military deception
MOB	mobile
MPT	manpower, personnel, and training

NAVNETWARCOM	Naval Network Warfare Command
NETCOM	Network Enterprise Technology Command (Army)
NSA	National Security Agency
NWS	network warfare squadron
NWW	network warfare wing
Ops	operations
PAF	Project AIR FORCE
PSYOP	psychological operations
RDT&E	research, development, test, and evaluation
SAF/XC	Secretary of the Air Force, Office of Warfighting Integration
SAF/XCI	Secretary of the Air Force, Office of Cyberspace Transformation and Strategy
SecAF	Secretary of the Air Force
SEI	special experience identifier
Spt	support
SQ	squadron
STRATCOM	United States Strategic Command
T&E	test and evaluation
Tech	technical
TNA	Telecommunications Network Attack
Trans Sys	transmission systems
TS	test squadron
TTP	tactics, techniques, and procedures
USSTRATCOM	United States Strategic Command
WG	wing

RAND PROJECT AIR FORCE

Human Capital Management for USAF Cyber Operations

DB579-1

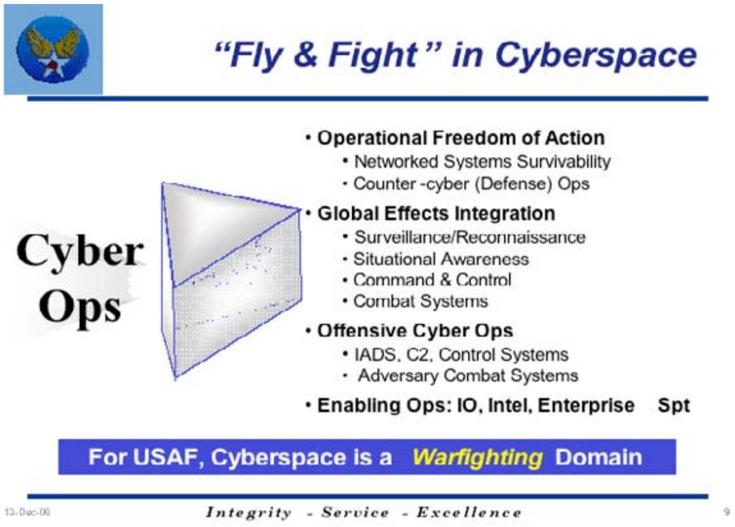
Introduction

On November 1, 2006, the Secretary of the Air Force and the Air Force Chief of Staff formally extended the Air Force's global vigilance, global reach, and global power into the cyberspace domain.[1] RAND was asked to identify and analyze the human capital management issues associated with the establishment of a formal cyberspace organization. This study was conducted when the Air Force's intent was to create a major command (MAJCOM) called AFCYBER to provide combat-ready forces trained and equipped to conduct sustained offensive and defensive global operations in and through cyberspace. By October 2008, the organizational construct for cyberspace capabilities had been revised to create a component numbered Air Force, 24th AF, within Air Force Space Command (AFSPC) that will focus on cyberspace warfighting operations.[2]

[1] Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers (JP 1-02).

[2] Our study focused on the human capital requirements for organizations that would be associated with the Air Force's cyber capabilities and was not affected by this revised organizational construct.

Air Force's Strategic Intent—Create a Warfighting Capability in Cyberspace



"Fly & Fight" in Cyberspace

Cyber Ops

- Operational Freedom of Action
  - Networked Systems Survivability
  - Counter -cyber (Defense) Ops
- Global Effects Integration
  - Surveillance/Reconnaissance
  - Situational Awareness
  - Command & Control
  - Combat Systems
- Offensive Cyber Ops
  - IADS, C2, Control Systems
  - Adversary Combat Systems
- Enabling Ops: IO, Intel, Enterprise Spt

For USAF, Cyberspace is a *Warfighting* Domain

13-Dec-06 *Integrity - Service - Excellence* 9

SOURCE: 8th AF, "Air Force Cyber Operations Command," briefing, December 13, 2006.

RAND Project AIR FORCE

DB579-2

Background

The *United States National Strategy to Secure Cyberspace* lists three objectives (Bush, 2003, p. viii): prevent cyber attacks against America's critical infrastructures; reduce national vulnerability to cyber attacks; and minimize damage and recovery time from cyber attacks that do occur. The National Military Strategy for Cyberspace Operations[3] further identifies the achievement of strategic superiority in cyberspace as a military objective (JCS, 2004, pp. 18, 23). With the advent of an organization dedicated to cyberspace operations, the Air Force initially planned to present cyber warfighting forces and capabilities to U.S. Strategic Command, geographical combatant commanders, and Joint task force commanders. Given these objectives, the Air Force identified the following desired end states (2006):

- Cyberspace attacks against vital U.S. interests deterred and prevented.
- Rapid response to attacks and reconstitution of networks should deterrence fail.
- Cyberspace power integrated into the full range of global effects.
- Adversaries operating through cyberspace defeated.
- Adversaries held at risk.

[3] Cyberspace operations include the employment of cyber capabilities whose primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid (JP 1-02).

- Assured availability of U.S. military networks.
- Persistent cyberspace situational awareness.

To help achieve these objectives, Headquarters United States Air Force (HAF) elements within warfighting integration (SAF/XC), cyber operations (AF/A3O-C), and manpower and personnel communities (AF/A1D and AF/A1P) pursued ways to either redesign existing career fields or create new career fields to support the human capital that would be designated as the Air Force's cyberspace force.

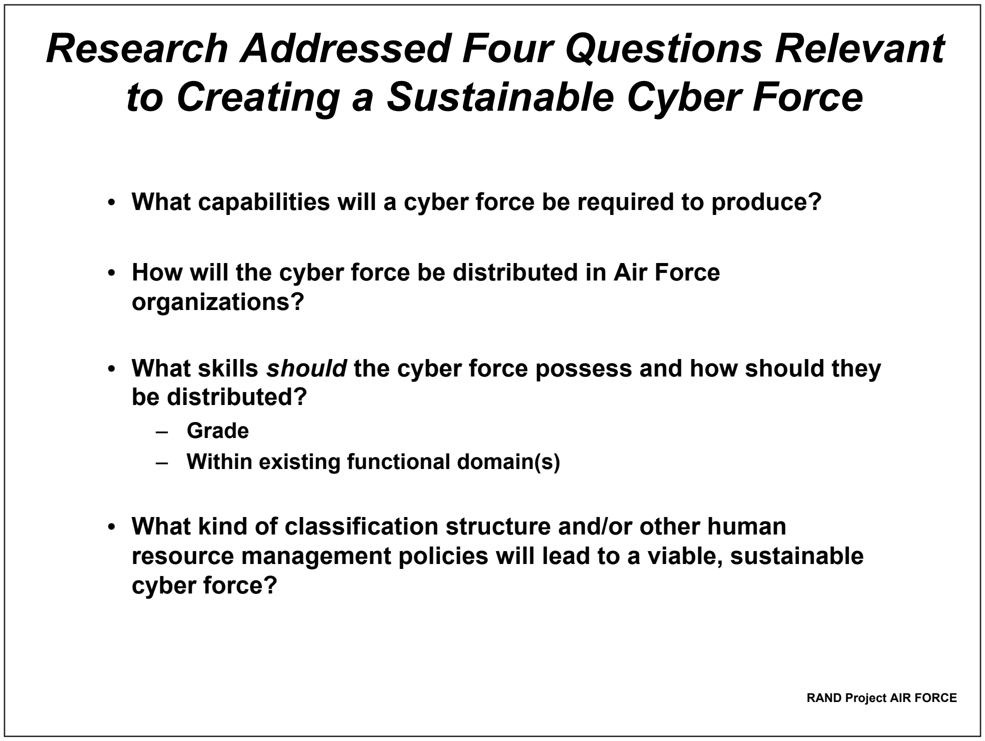
The Secretary of the Air Force, Office of Cyberspace Transformation and Strategy (SAF/XCI) has functional management responsibilities for the communications and computer career fields.[4] This office was primarily concerned with identifying future development requirements for airmen in the communications-computer career field who would make up a significant portion of the cyberspace force. It was also interested in whether emerging cyber capabilities would affect development requirements for other participating career fields, such as information operations (IO) and command and control, intelligence, surveillance, and reconnaissance (C2ISR).

AF/A3O-C has functional management responsibilities for the IO career field. This office wanted to understand how the skill requirements of airmen engaged in IO and the management of IO-qualified airmen should be integrated in the emerging cyber force.

The directorates of Force Management Policy (AF/A1P) and Airman Development and Sustainment (AF/A1D) were interested in the skill development and force management implications of creating a cyber force from the existing Air Force inventory.

The study's design was influenced by our assessment of the various needs seen by these offices. We concluded that the analyses needed to (1) be strategically oriented, identifying the human capital requirements to which a new cyberspace organization would likely evolve; (2) be comprehensive, considering human capital requirements driven by envisioned Air Force cyber capabilities, and possibly by other services and agencies; and (3) produce insights about how to design effective force management and development policies.

[4] These career fields include the 33S Communications Officer specialty and nine enlisted specialties: 2E0, Ground Radar; 2E1, Satellite Communication/Wideband/Telemetry/Meteorological/Radio Imagery and Intrusion; 2E2, Communication/Network/Switching and Cryptographic Systems; 2E6, Cable/Antenna/Telephony; 3A0, Information Management; 3C0, Communications-Computer Operators and Programmers; 3C1, Radio/Spectrum Operators; 3C2, Communications-Computer Systems Controllers; and 3C3, Communications-Computer Plans/Implementation.



Research Addressed Four Questions Relevant to Creating a Sustainable Cyber Force

- **What capabilities will a cyber force be required to produce?**
- **How will the cyber force be distributed in Air Force organizations?**
- **What skills *should* the cyber force possess and how should they be distributed?**
  - **Grade**
  - **Within existing functional domain(s)**
- **What kind of classification structure and/or other human resource management policies will lead to a viable, sustainable cyber force?**

RAND Project AIR FORCE

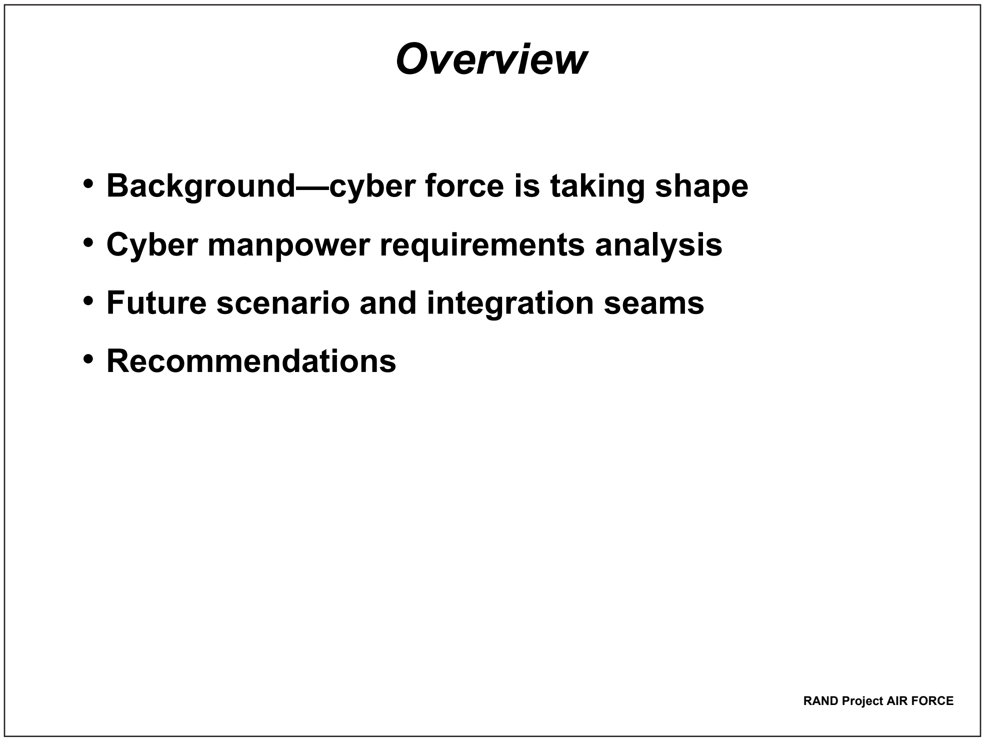
DB579-3

Research Questions

The research addressed four questions relevant to creating a sustainable cyber force. First, the requirements for human capital should be predicated upon the cyber capabilities that the Air Force intends to produce. This question is consistent with a top-down approach to determining human capital requirements. When human capital requirements are derived from the characterization of end-state capabilities, alignments between estimates of human capital requirements and organizational outcomes are likely to be more specific. Therefore, we sought detailed descriptions of envisioned cyber capabilities at the unclassified level from subject-matter experts. Second, cyber personnel are likely to be required in different kinds of organizations—ranging from those that produce cyber effects to those that provide functional support to cyber effects–generating organizations. Although Air Force cyber personnel will be made available to combatant commanders and other government agencies, the Air Force had not yet specified how these positions would be allocated to these organizations. Therefore, we focused on where these positions are likely to be distributed within Air Force organizations.[5] Third, since the Air Force's cyber capabilities are still emerging, we sought to identify the skills that a fully functioning cyber force should possess and where those skills should reside across the Air Force rank structure and within current functional communities. Answers to the first three questions were intended to provide the grounding to address suitable approaches to managing a cyber force. Fourth, the Air Force was particularly interested in identifying a

[5] Air Force units train and equip the forces the Air Force provides to combatant commanders and other governmental agencies.

classification structure and force management policy that would lead to a technically proficient, operationally relevant, sustainable force. Our research evaluated different approaches to managing a viable and sustainable force in the interest of informing policy options that were then under consideration.



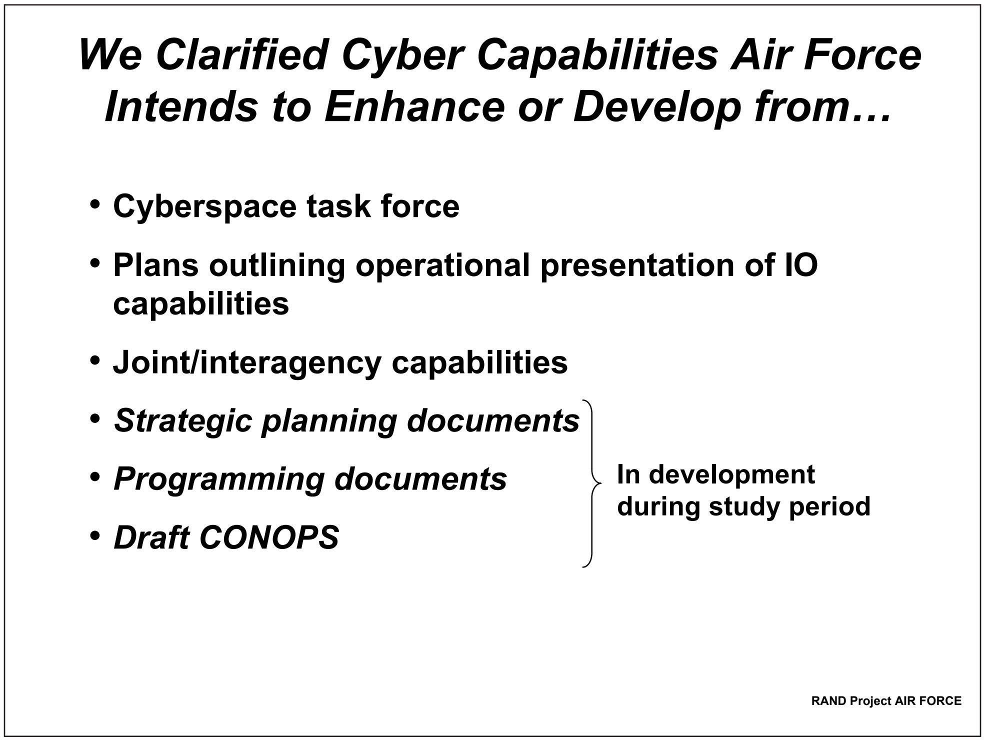
Overview

- Background—cyber force is taking shape
- Cyber manpower requirements analysis
- Future scenario and integration seams
- Recommendations

RAND Project AIR FORCE

DB579-4

This documented briefing reports our findings. First, we describe how the conceptualization of a cyber force was taking place during the time frame of the study, from October 2006 through September 2007. Next, we present answers to the research questions with a specific focus on the Air Force occupational specialties most affected by the emerging cyber mission. Since cyberspace capabilities are constantly evolving, we also provide a perspective on the cyber future the Air Force might confront and its potential implications for how the Air Force manages its cyber force. Finally, we provide recommendations.



We Clarified Cyber Capabilities Air Force Intends to Enhance or Develop from…

- **Cyberspace task force**
- **Plans outlining operational presentation of IO capabilities**
- **Joint/interagency capabilities**
- ***Strategic planning documents***
- ***Programming documents***
- ***Draft CONOPS***

In development during study period

RAND Project AIR FORCE

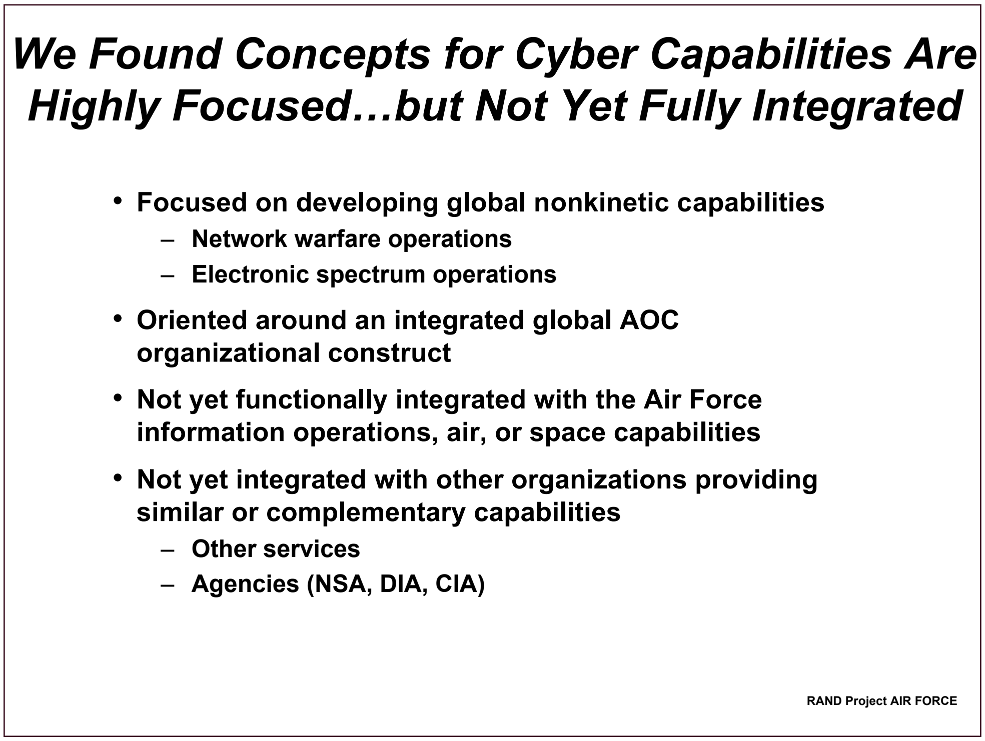
DB579-5

The Cyber Force Is Taking Shape

Strategic Review of the Air Force's Envisioned Capabilities

We sought to clarify the capabilities that the Air Force intends to enhance or develop. Our first source was the Air Force's Cyberspace Task Force. The Secretary of the Air Force (SecAF) and Chief of Staff of the Air Force (CSAF) established this task force to conduct the initial planning and coordination needed to operationalize a vision for "flying and fighting" in cyberspace. In meetings with task force members, we gleaned information about the Air Force's reasons for defining the mission area, its envisioned cyber capabilities, and the planning stages that would lead to an initial operating capability of a cyber command. Cyberspace operations have historically been within IO doctrine (see, e.g., Joint Publication 3-13, *Information Operations*) where, in particular, computer network operations are listed as one of five core capabilities.[6] Therefore, prior Air Force IO plans and current Joint IO plans were another source of information about cyber capabilities. Doctrine and supporting documents outlined the scope of capabilities that could fall within the Air Force's cyber mission area. Unclassified descriptions of current Joint and interagency cyber capabilities helped us understand the techniques comprising the Air Force's current—and potential—cyber capabilities. At the time of this research, strategic planning documents, programming documents, and concept of operations (CONOPS) documents were in development and coordination. These sources of information provided a window into the capabilities that the Air Force planned to develop and how those capabilities would be integrated operationally.

[6] The other four are electronic warfare, psychological operations, operations security, and military deception.



We Found Concepts for Cyber Capabilities Are Highly Focused…but Not Yet Fully Integrated

- Focused on developing global nonkinetic capabilities
  - Network warfare operations
  - Electronic spectrum operations
- Oriented around an integrated global AOC organizational construct
- Not yet functionally integrated with the Air Force information operations, air, or space capabilities
- Not yet integrated with other organizations providing similar or complementary capabilities
  - Other services
  - Agencies (NSA, DIA, CIA)

RAND Project AIR FORCE

DB579-6

Our findings from this strategic-level review are twofold. First, the Air Force's conceptualizations of how to "fly and fight" in cyberspace are highly focused on network warfare operations and electronic spectrum operations that can be integrated with current and future kinetic capabilities.

- Network warfare operations consist of network attack, network defense, and network support capabilities. Network attack consists of airborne and ground-based capabilities that will hold an adversary at risk across air, space, cyberspace, land, and maritime domains. Network defense capabilities consist of threat analysis, operational preparation of the battlefield, and active defense of computer networks. Network support consists of the capabilities to establish network operations globally and provide assurance of networks in different threat environments (DAF, 2005).
- Electronic spectrum operations use electromagnetic or directed energy to manipulate the electromagnetic spectrum or attack an adversary. Examples include electromagnetic jamming and deception, spectrum management and electromagnetic hardening, and electromagnetic threat warning (JP 3-13.1).[7]

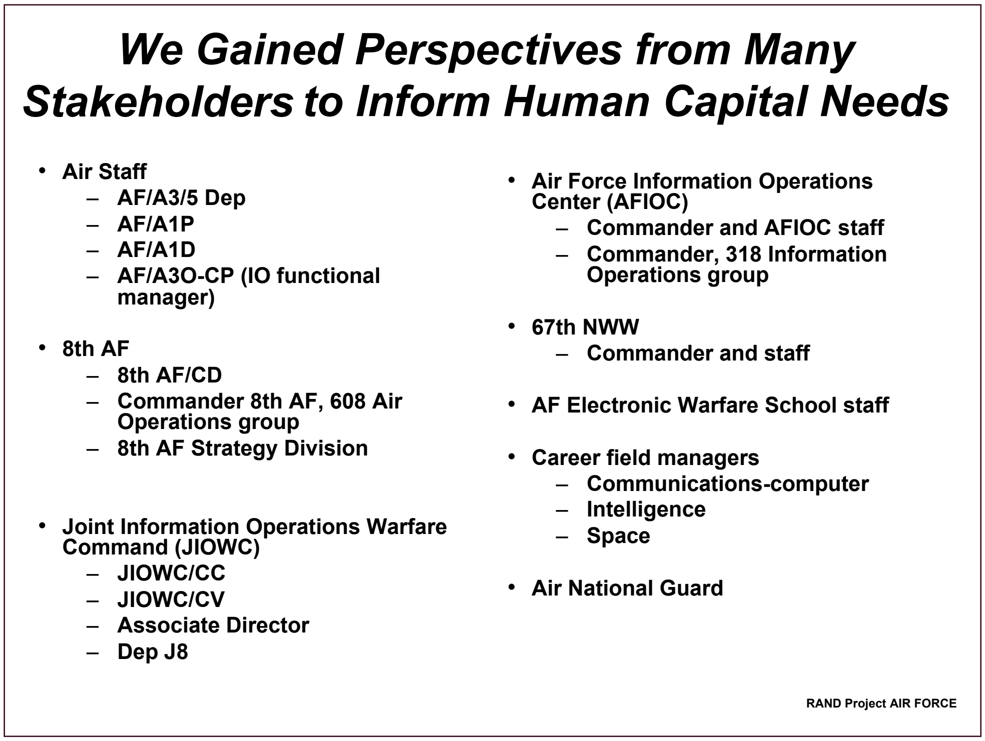
The Air Force envisions that warfighting cyber capabilities either will be employed as a stand-alone, nonkinetic strike capability or will be used in concert with kinetic capabilities and would be operationally integrated through a global Air Operations Center (AOC). Achieving the goal for combined kinetic and nonkinetic strike capability will also depend on the functional integration of cyber capabilities with existing IO, air, and space capabilities. Such inte-

[7] This class of operations has to do with manipulating the electromagnetic spectrum to improve aircraft survivability or attack an adversary's targets.

gration would allow for accurate assessments of effective single uses of nonkinetic capability or the most effective combination and sequencing of specific cyber and kinetic capabilities. However, at the time of this research, the Air Force had not specified how such functional integration would take place or what effects would be produced from that integration.

Our second finding addresses external integration. The Air Force is not the only organization developing capabilities to operate effectively in cyberspace. However, at the time of this research we found no evidence of substantive planning for integrating its envisioned capabilities with other organizations providing similar or complementary capabilities. For example, the Army organizes, trains, and equips its information assurance and network defense capabilities within its Network Enterprise Technology Command (NETCOM), commanded by a major general. The comparable Navy organization responsible for computer network operations is the Naval Network Warfare Command (NAVNETWARCOM), commanded by a vice admiral. Since Air Force capabilities contribute to joint missions, it is reasonable to expect that the planning for development and employment of Air Force cyber capabilities would address integration with other services' efforts. Moreover, intelligence plays a critical role for effective network operations and electronic spectrum operations. Several defense agencies also have important, existing roles that seem to overlap the Air Force's planned capabilities.[8] However, we found no evidence that planning efforts aim to integrate these organizations' capabilities with the Air Force's approach for creating and delivering cyber effects.

[8] The National Infrastructure Protection Center within the Department of Homeland Security is tasked with detecting, averting, assessing, warning against, responding to, and investigating unlawful acts that target or threaten critical infrastructures in general and computer and information technologies in particular. The National Security Agency and the Defense Information Systems Agency have collaborative responsibilities to provide battlespace visibility and situational impacts; identify network attack impacts; and perform consequence management and response. The other military services and the Federal Bureau of Investigation (FBI) are also developing cyber programs that seem relevant.



We Gained Perspectives from Many Stakeholders to Inform Human Capital Needs

- Air Staff
  - AF/A3/5 Dep
  - AF/A1P
  - AF/A1D
  - AF/A3O-CP (IO functional manager)
- 8th AF
  - 8th AF/CD
  - Commander 8th AF, 608 Air Operations group
  - 8th AF Strategy Division
- Joint Information Operations Warfare Command (JIOWC)
  - JIOWC/CC
  - JIOWC/CV
  - Associate Director
  - Dep J8
- Air Force Information Operations Center (AFIOC)
  - Commander and AFIOC staff
  - Commander, 318 Information Operations group
- 67th NWW
  - Commander and staff
- AF Electronic Warfare School staff
- Career field managers
  - Communications-computer
  - Intelligence
  - Space
- Air National Guard

RAND Project AIR FORCE

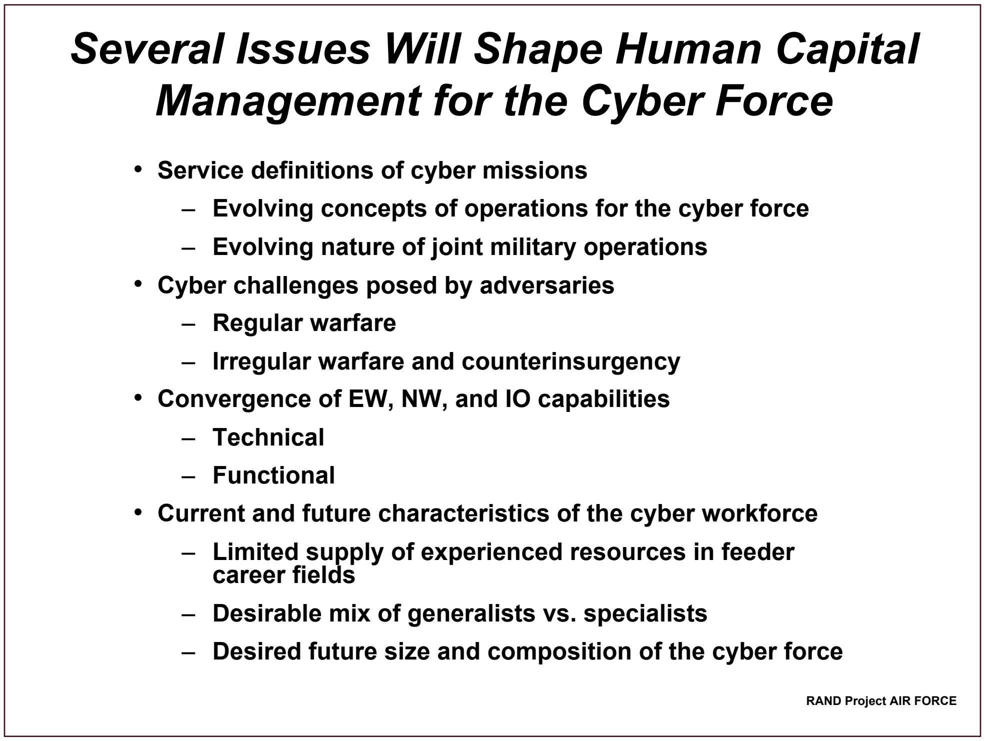
DB579-7

Cyber Human Capital Management Practices and Issues

We obtained information about the Air Force's current and planned cyber capabilities from a variety of organizations that were influencing the plans for organizing MAJCOM-level cyber capabilities. Our questions to the leaders in these organizations and their staff focused on the human capital implications for cyberspace organization. These interviews highlighted many issues for consideration.

Air Staff–level interviews surfaced the challenges of crafting the full suite of operational cyber capabilities within a constrained resource environment while simultaneously trying to identify the personnel who could make up the initial cyber cadre. Leaders and staff at 8th Air Force discussed the early stages of CONOPS development but admitted that human capital management strategies had not yet been fully thought through. Staff at the Joint Information Operations Warfare Command (JIOWC) described how the Air Force's intent to create a cyber-focused MAJCOM did not appear to acknowledge current IO doctrine and failed to identify the skill sets in influence operations that some segment of a cyber force should possess. Our interviews with leaders and staff at the Air Force Information Operations Center (AFIOC), the 67th Network Warfare Wing (NWW), and the Air Force Electronic Warfare School focused on the current training, manning, and operational issues of current IO and cyber-related operations. Discussions ranged from the importance of creating cyber human capital that is both technically and operationally proficient to problems of inadequate manning in some organizations and inadequate depth in critical cyber skills among assigned personnel.

Initial planning documents for proposed organization identified the communications-computer, intelligence, and space career fields as major contributors to the envisioned cyber force. Interviews with the respective career field managers surfaced numerous human capital management issues, including (1) how recent strength reductions in the communications-computer career field were at odds with the enlargement of cyber capabilities that would largely rely on that career field; (2) how intentions to integrate portions of the intelligence career field were at odds with the Air Force's ongoing initiative to strengthen intelligence (A2) capabilities and provide focused career development for intelligence personnel; and (3) how the reasoning was unclear for the inclusion of space personnel as part of the cyber human capital pool. Interviews with the Air National Guard surfaced the human capital skill sets that guard and reserve forces contribute to current capabilities and how those forces could help the Air Force retain access to key skill sets.



Several Issues Will Shape Human Capital Management for the Cyber Force

- **Service definitions of cyber missions**
  - **Evolving concepts of operations for the cyber force**
  - **Evolving nature of joint military operations**
- **Cyber challenges posed by adversaries**
  - **Regular warfare**
  - **Irregular warfare and counterinsurgency**
- **Convergence of EW, NW, and IO capabilities**
  - **Technical**
  - **Functional**
- **Current and future characteristics of the cyber workforce**
  - **Limited supply of experienced resources in feeder career fields**
  - **Desirable mix of generalists vs. specialists**
  - **Desired future size and composition of the cyber force**

RAND Project AIR FORCE

DB579-8

Our synthesis of the information gathered from these stakeholders identified several issues that will likely shape human capital management of the cyber force. They can be grouped into four categories. First, the requirements for human capital will be influenced by the military services' definitions of how they will operate in cyberspace. Capabilities that are delivered through, or rely on, the electromagnetic spectrum will continue to increase in frequency, sophistication, and along the spectrum of conflict. The Air Force's specification of the scope of defensive operations, offensive operations, and network exploitation, and how those operational capabilities will be presented across the spectrum of conflict can affect the size of the cyber force and the skills it possesses. For example, the levels of cyber vulnerability to defend, attack, or exploit range from applying strategies and techniques to protect high-level processes and relationships, such as command and control, to protecting functional systems and the vulnerabilities of supporting technologies. Aligning operations at each level requires personnel who possess specific skill and knowledge sets. Consequently, the number of defense, attack, or exploitation levels the cyber force includes within in its concept of operations could influence its size. Moreover, the Air Force operates in a Joint environment and each service has developed cyber capabilities. As the nature of Joint operations and related cyber operations evolves, so may the specification of size and skill requirements of Air Force cyber personnel.

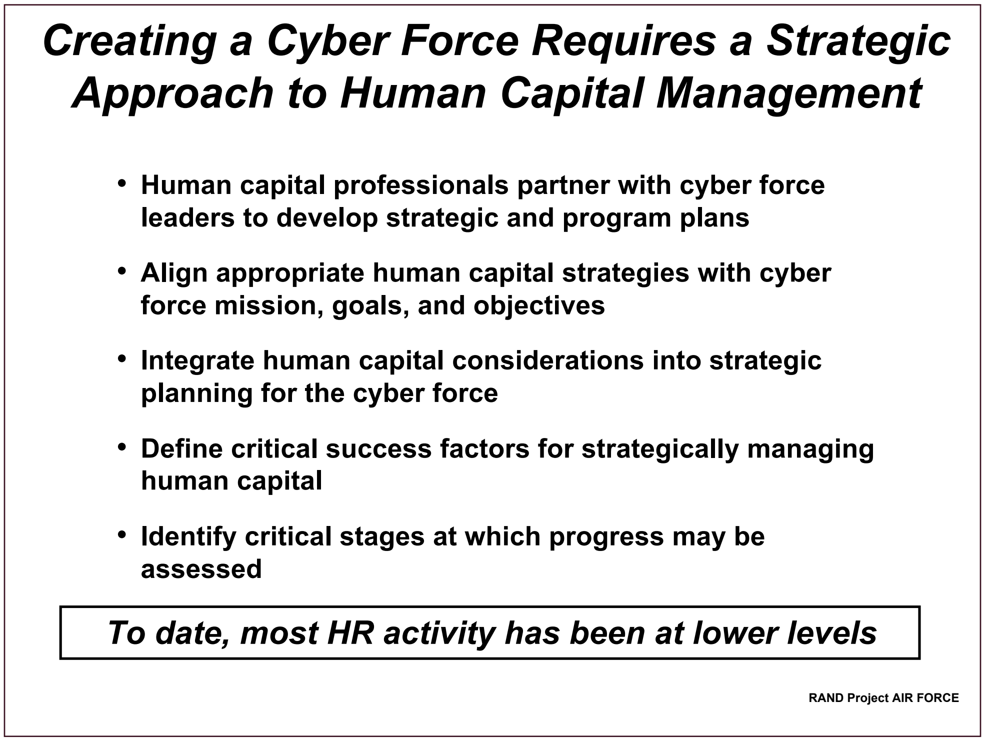
Second, cyber threats posed by current and potential adversaries will shape the need for the Air Force to create agile strategies and capabilities to counter such threats. There is evidence that nation-state actors are actively developing cyber-based capabilities for network exploitation and network attack. The Air Force has to organize, train, and equip its cyber force to successfully prevail in any number of traditional warfare scenarios. But cyber warfare capabilities are also the tools of non-state actors. IW and counterinsurgency actions against coalition forces in Iraq and Afghanistan have often incorporated the use of information technology and the electromagnetic spectrum as a means of influence, organization, and attack. An Air Force cyber force will need the skills to develop and employ cyber capabilities that mitigate or eliminate the likely increasing use of cyber-based tools and techniques in this kind of warfare most closely associated with the Global War on Terrorism.

Third, the rapid evolution of information technology (IT) is expected to shape cyber human capital management. For example, advances in the capacity, speed, and application of information technology are likely to result in

- new electronic warfare (EW) methods to use and control the electromagnetic spectrum
- rapid evolution of network warfare techniques and tools to attack and defend networked computers and supporting IT infrastructures using the electromagnetic spectrum
- the creation of IO techniques and tools, particularly influence operations, that leverage the effects generated by EW and net warfare.

Such advances could enlarge the scope of operational skills and experience that Air Force cyber warriors should possess to ensure technical superiority against potential adversaries.

The final category is the characteristics of the current cyber workforce and how it compares with the desired characteristics of the workforce of the future. Currently, the targeted feeder career fields have small cadres of people, certified by the National Security Agency (NSA) and commercial IT certification organizations, who possess the requisite skills that are needed to produce the capabilities envisioned by the Air Force. If the Air Force identifies shortfalls in skilled cyber personnel, then aggressive human capital management strategies may be needed to increase the pool of certified personnel for computer network defense, computer network attack, and computer network exploitation. A related issue is the mix of cyber generalists and cyber specialists the Air Force needs in cyberspace organizations. Generalists would have broader experience with the operational application of cyber capabilities; specialists would have expertise with specific information technologies, infrastructures, tools, and codes. The Air Force's specification of the mix will influence how the cyber force is selected, trained, and developed. Future size objectives could signal the need for human capital management strategies that adjust sustainability targets for the career force and influence retention dynamics. Also, officers and enlisted personnel from the active and reserve components, as well as civilians, will constitute the human capital for the planned organization. Decisions about the total force composition will influence human capital management strategies for the organization as well.



Creating a Cyber Force Requires a Strategic Approach to Human Capital Management

- Human capital professionals partner with cyber force leaders to develop strategic and program plans
- Align appropriate human capital strategies with cyber force mission, goals, and objectives
- Integrate human capital considerations into strategic planning for the cyber force
- Define critical success factors for strategically managing human capital
- Identify critical stages at which progress may be assessed

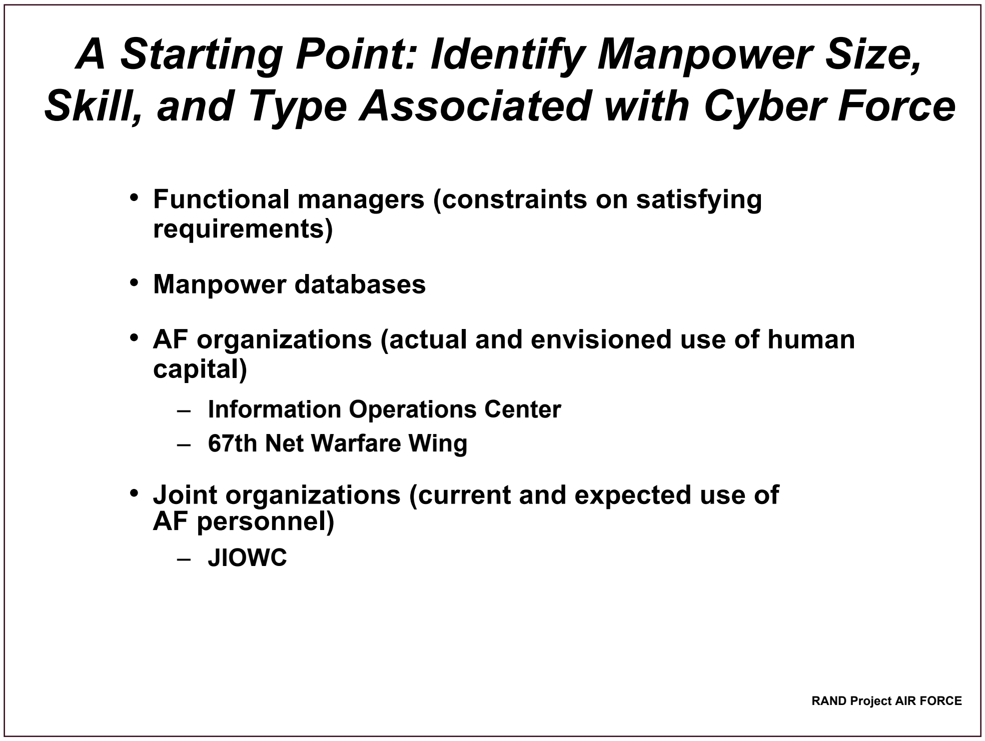
To date, most HR activity has been at lower levels

RAND Project AIR FORCE

DB579-9

A Strategic Approach to Human Capital Management Is Warranted

Having considered the numerous issues, we concluded that the Air Force needs to adopt a strategic approach to human capital management as it builds its cyber force. At the time of this research, the Air Force's human capital planning activity was focused at the tactical level—exploring ways to establish a new cyber Air Force Specialty Code (AFSC) and establishing and coordinating the rules that would identify who, within the current force, would be awarded the new AFSC. Although these activities and decisions are important, they do not address what human capital parameters need to be satisfied to support the operational and strategic objectives for cyber capabilities. A strategic approach to human capital management would follow five broad steps: First, the career field managers and human capital professionals in AF/A1 would partner with cyber force leaders in AF/A3/5 and existing cyber organizations to develop strategic programs and plans. The primary objective would be to align appropriate human capital strategies with the mission, goals, and objectives of the cyberspace organization. This activity would focus human capital planning on the core capabilities and needs of the planned organization. Next, human capital selection, development, utilization, and sustainment should be integrated with the operational planning for a cyber force. Integration of these considerations at this early stage increases the likelihood that human capital will be evaluated on a par with other resource requirements. Finally, critical success factors that are instrumental to achieving the long-term size, skill, and composition goals for the cyber force should be identified. Examples include achieving the required recruiting and retention levels of cyber personnel with critical skills needed to sustain a career force; achieving the desired ratios of active duty, reserve component, and civilian personnel in the cyber force; and identifying the critical stages at which progress toward these objectives should be assessed.



A Starting Point: Identify Manpower Size, Skill, and Type Associated with Cyber Force

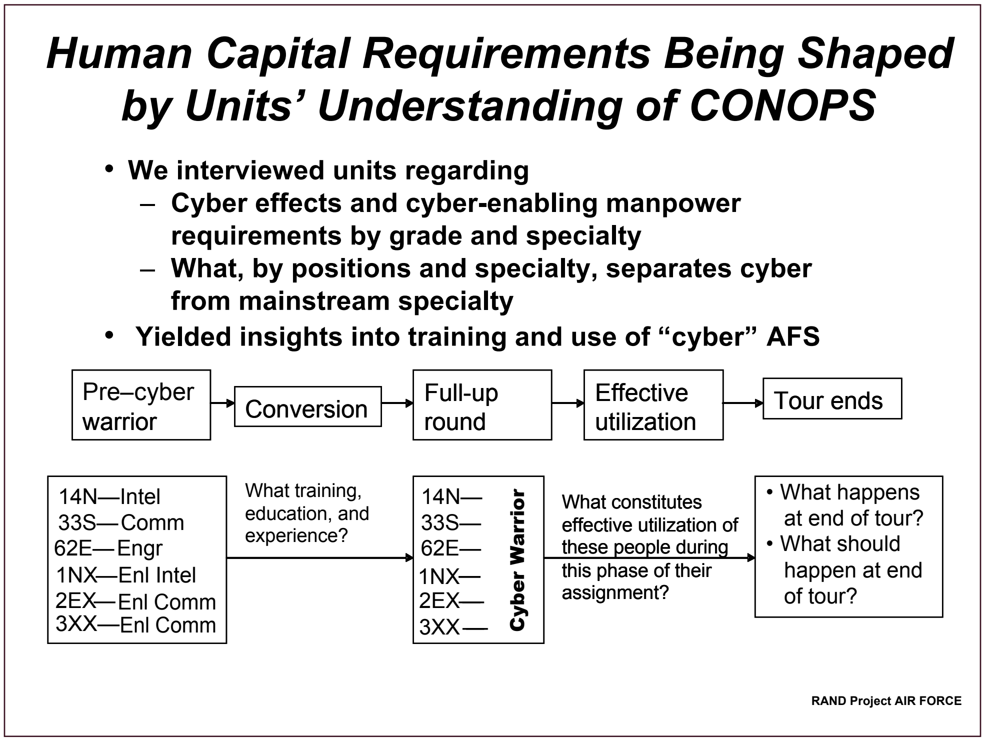
- **Functional managers (constraints on satisfying requirements)**
- **Manpower databases**
- **AF organizations (actual and envisioned use of human capital)**
  - **Information Operations Center**
  - **67th Net Warfare Wing**
- **Joint organizations (current and expected use of AF personnel)**
  - **JIOWC**

RAND Project AIR FORCE

DB579-10

Cyber Manpower Requirements Analysis

As a starting point, we identified the size, types, and skills of the manpower currently associated with the cyber force. Our information and data came from managers of the functional communities currently engaged in cyber activities. They provided a comprehensive understanding of where and how personnel were being used as cyber assets. They also informed us about any existing constraints (e.g., career field sustainability, or conflicting mission requirements) on their community's capability to satisfy the envisioned human resource (HR) requirements for the planned organization. We developed estimates of demand for cyber human capital from manpower databases that revealed the current requirement for cyber personnel by organization, Air Force specialty, and grade. We gathered additional data about current and envisioned demand from on-site visits to a small sample of cyber and IO organizations, all located at Lackland Air Force Base: the AFIOC, the 67th NWW, and the JIOWC.



Human Capital Requirements Being Shaped by Units' Understanding of CONOPS

- We interviewed units regarding
  - Cyber effects and cyber-enabling manpower requirements by grade and specialty
  - What, by positions and specialty, separates cyber from mainstream specialty
- Yielded insights into training and use of "cyber" AFS

Pre–cyber warrior → Conversion → Full-up round → Effective utilization → Tour ends

14N—Intel
33S—Comm
62E—Engr
1NX—Enl Intel
2EX—Enl Comm
3XX—Enl Comm

What training, education, and experience?

14N—
33S—
62E—
1NX—
2EX—
3XX—
Cyber Warrior

What constitutes effective utilization of these people during this phase of their assignment?

- What happens at end of tour?
- What should happen at end of tour?

RAND Project AIR FORCE

DB579-11

Developing "Full-Up Round" Cyber Warriors

After examining these data and information, we recognized that the human capital requirements for cyber and cyber-related organizations are currently being shaped at the unit level. Organizations that contribute to the creation of cyber effects operate from their unit-specific interpretation of a CONOPS for either cyber or IO capabilities. Each organization, however, shared the same approach to developing human capital. Typically, personnel assigned to the AFIOC, the 67th NWW, and the JIOWC arrive with limited network warfare or IO experience. In many cases, assignments to these organizations are considered as broadening tours that are off the traditional career trajectory within the functional community. Among officers, the pre–cyber warrior typically comes from the intelligence (AFSC 14N), communications-computer (AFSC 33S), or developmental engineering (AFSC 62E) functional community.[9] Enlisted pre–cyber warriors are also from the intelligence (AFSC 1NX) and communications-computer (AFSCs 2EX and 3CX) functional communities. Each organization reported that most new personnel arrive with skills from their primary specialty and are converted into "full-up round" cyber warriors through training, education, and experience over a six- to eight-month period. After their on-the-job training (OJT) is completed, they may satisfy the requirements for a variety of positions in the organization.

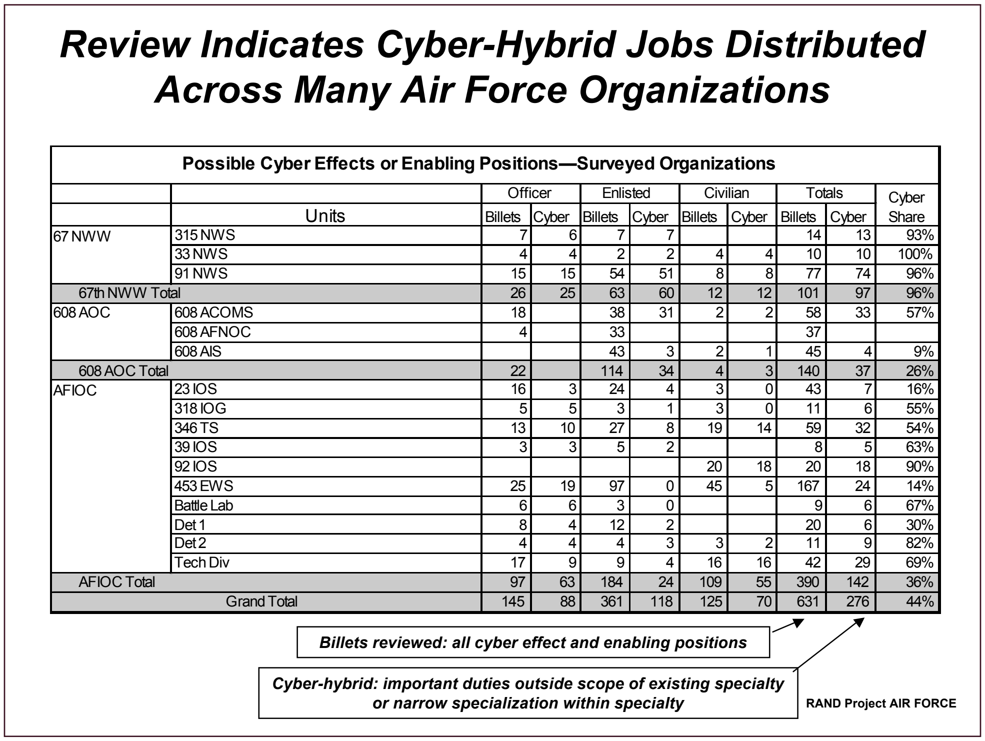
The description of this process prompted three questions regarding human capital management:

[9] Our analysis focused on organizations whose missions were most closely correlated to cyber attack, cyber defense, and cyber exploitation. These organizations did not contain several cyber-related C2ISR and IO specialties, such as 11R, 11U, 12R, 12U, 13B, 13S for officers and 1A3, 1A4, 1C2, 1C5, 1C6, and 2A3 for enlisted personnel.

- What types of training, education, and experience are necessary to produce an effective conversion?
- What constitutes effective utilization of “full-up rounds” during their assignments?
- How can these experienced cyber warriors be effectively used after their tours end?

To answer these questions, we conducted a position review for a sample of organizations that were either responsible for producing cyber effects or produced capabilities that enabled the production of cyber effects. The sample included organizations where we had conducted earlier site visits and additional organizations such as the 608th AOC. The review excluded each organization’s staff positions and contained details on personnel by grade and Air Force specialty. We asked whether positions required cyber-specific skills that were beyond the domain of the specialty assigned to the position and whether the skills an incumbent gained in various positions could be used either in other cyber-related organizations or in non–cyber-related Air Force organizations. The responses were expected to yield insights regarding the following questions: (1) How many positions in these organizations require cyber-hybrid skills—combinations of the mainstream specialty’s skills and specific cyber skills gained through OJT?[10] (2) What training needs are common across cyber-hybrid positions? (3) Can the hybrid skills be used in other tours? (4) Would a new Air Force cyber specialty be the most effective way to manage this human capital?

[10] *Mainstream specialty* refers to the Air Force specialty coded to the position.



Review Indicates Cyber-Hybrid Jobs Distributed Across Many Air Force Organizations

Possible Cyber Effects or Enabling Positions—Surveyed Organizations

		Officer		Enlisted		Civilian		Totals		Cyber
	Units	Billets	Cyber	Billets	Cyber	Billets	Cyber	Billets	Cyber	Share
67 NWW	315 NWS	7	6	7	7			14	13	93%
	33 NWS	4	4	2	2	4	4	10	10	100%
	91 NWS	15	15	54	51	8	8	77	74	96%
67th NWW Total		26	25	63	60	12	12	101	97	96%
608 AOC	608 ACOMS	18		38	31	2	2	58	33	57%
	608 AFNOC	4		33				37		
	608 AIS			43	3	2	1	45	4	9%
608 AOC Total		22		114	34	4	3	140	37	26%
AFIOC	23 IOS	16	3	24	4	3	0	43	7	16%
	318 IOG	5	5	3	1	3	0	11	6	55%
	346 TS	13	10	27	8	19	14	59	32	54%
	39 IOS	3	3	5	2			8	5	63%
	92 IOS					20	18	20	18	90%
	453 EWS	25	19	97	0	45	5	167	24	14%
	Battle Lab	6	6	3	0			9	6	67%
	Det 1	8	4	12	2			20	6	30%
	Det 2	4	4	4	3	3	2	11	9	82%
	Tech Div	17	9	9	4	16	16	42	29	69%
AFIOC Total		97	63	184	24	109	55	390	142	36%
	Grand Total	145	88	361	118	125	70	631	276	44%

Billets reviewed: all cyber effect and enabling positions

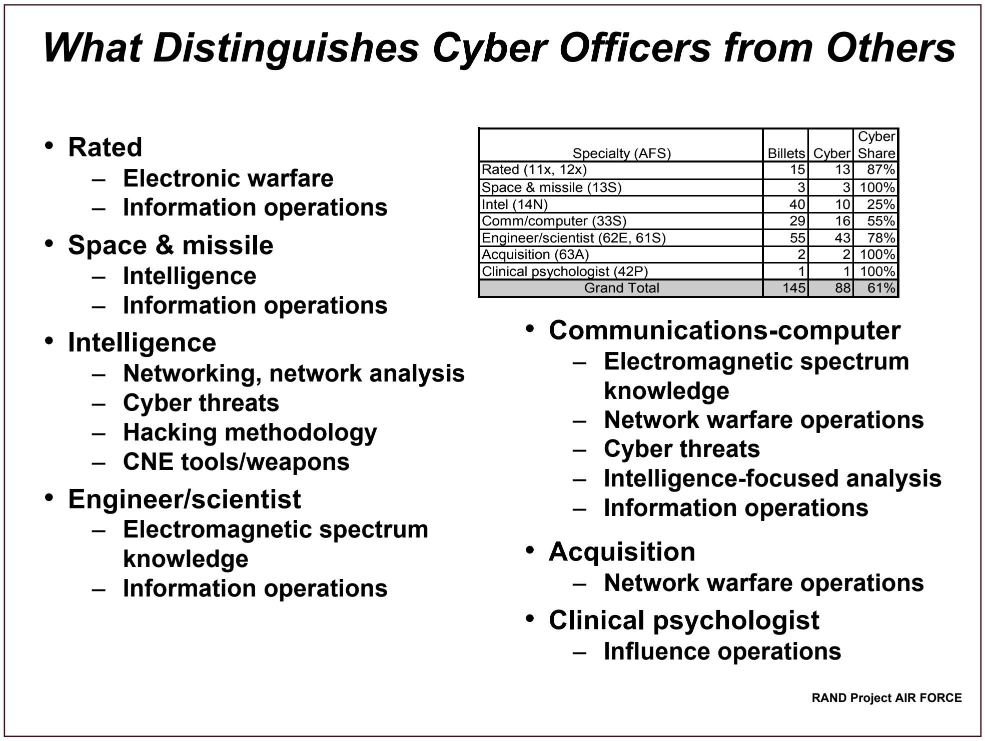
Cyber-hybrid: important duties outside scope of existing specialty or narrow specialization within specialty

RAND Project AIR FORCE

DB579-12

Air Force Cyber-Hybrid Jobs

Our analysis focuses on the cyber-hybrid requirements in Air Force organizations. The first finding from the position review is that cyber-hybrid jobs are distributed across the 67th NWW, the 608th AOC, and the AFIOC. The 67th NWW is a cyber effects–generating organization with officer, enlisted, and civilian billets, the majority requiring cyber-hybrid skills. The 608th AOC is a cyber-enabling organization that incorporates the Air Force Network Operations Center (AFNOC), the 608th Air Intelligence Squadron, and the 608th Air Communications Squadron (ACOMS). These organizations are manned predominantly by enlisted personnel. Most of the cyber-hybrid positions are found in the 608th ACOMS, where 33 out of 58 positions were identified as requiring cyber-hybrid skills. No positions in the AFNOC were reported to require cyber-hybrid skills and only four of 45 positions in the 608th Air Intelligence Squadron (AIS) required cyber-hybrid skills. The AFIOC comprises cyber effects-generating organizations and cyber-enabling organizations that have officer, enlisted, and civilian positions. Each AFIOC organization's mission determines the size of the cyber-hybrid position requirements. For example, higher proportions exist in the 346th Test Squadron (32 of 59), the 92nd Information Operations Squadron (18 of 20), and the Technology Division (29 of 42). In total, nearly 44 percent (276 of 631) of the positions across these organizations were specified as having cyber-hybrid skill requirements.



What Distinguishes Cyber Officers from Others

- **Rated**
  - **Electronic warfare**
  - **Information operations**
- **Space & missile**
  - **Intelligence**
  - **Information operations**
- **Intelligence**
  - **Networking, network analysis**
  - **Cyber threats**
  - **Hacking methodology**
  - **CNE tools/weapons**
- **Engineer/scientist**
  - **Electromagnetic spectrum knowledge**
  - **Information operations**

Specialty (AFS)	Billets	Cyber	Cyber Share
Rated (11x, 12x)	15	13	87%
Space & missile (13S)	3	3	100%
Intel (14N)	40	10	25%
Comm/computer (33S)	29	16	55%
Engineer/scientist (62E, 61S)	55	43	78%
Acquisition (63A)	2	2	100%
Clinical psychologist (42P)	1	1	100%
Grand Total	145	88	61%

- **Communications-computer**
  - **Electromagnetic spectrum knowledge**
  - **Network warfare operations**
  - **Cyber threats**
  - **Intelligence-focused analysis**
  - **Information operations**
- **Acquisition**
  - **Network warfare operations**
- **Clinical psychologist**
  - **Influence operations**

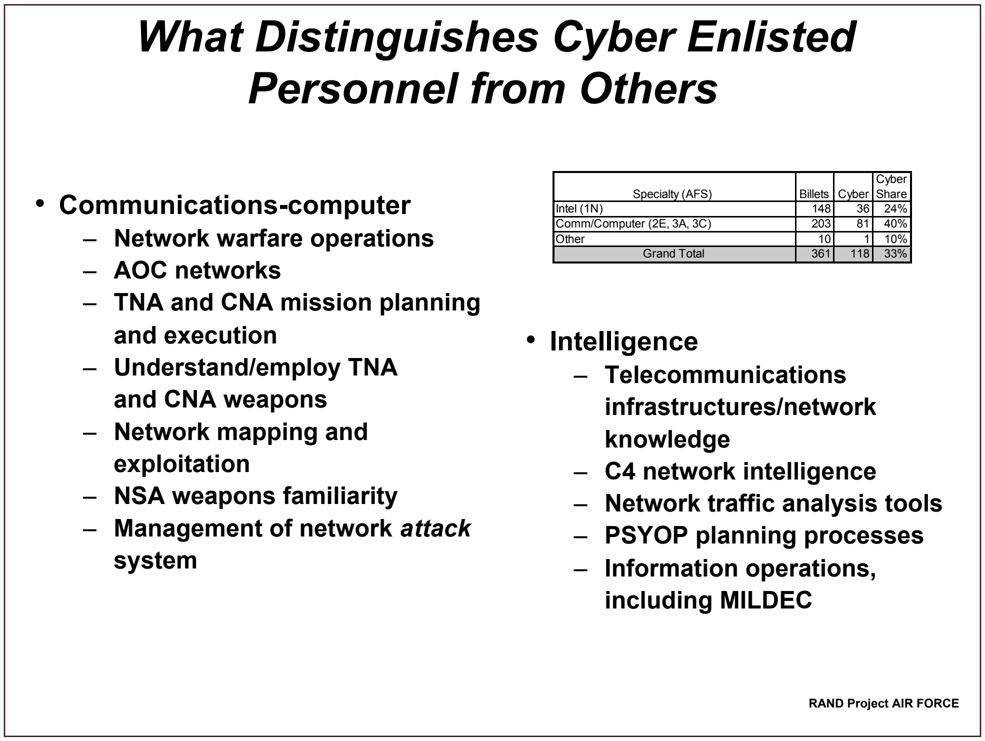
RAND Project AIR FORCE

DB579-13

Our more detailed analysis of these cyber-hybrid skills is presented here. The 67th NWW, 608th AOC, and the AFIOC have 145 officer billets distributed across seven officer specialties. Among the billets with cyber-hybrid skill requirements, we drilled down further to identify the specific cyber skill areas that were needed for each specialty.[11] Most of the rated officer positions (13 of 15) were identified as requiring additional skills in electronic warfare and information operations. The three positions requiring space and missile specialties each required augmentation with intelligence and IO skills. Among the 40 intelligence officer positions in these organizations, ten required incumbents to possess augmenting skills in networking and network analysis, cyber threats, hacking methodology, and/or computer network exploitation tools and weapons. Higher proportions of communications-computer officer positions (16 of 29) required additional skills in the areas of electromagnetic spectrum knowledge, network warfare operations, knowledge of cyber threats, and/or IO. Developmental engineer and scientist positions, largely found in the AFIOC, also required electromagnetic spectrum knowledge and/or IO skills. Even acquisition officer positions and the lone clinical psychologist billet called for additional cyber skills. Acquisition officers needed knowledge in network warfare operations, and the clinical psychologist required additional knowledge in influence operations.

[11] It is worth noting that RAND's research addressing the officer force above O-5 identified IO and/or C2ISR as secondary or paired skills for important numbers of rated, space, intelligence, and communications officers (for example, see Robbert et al., 2004).

In total, 88 of 145 officer billets (61 percent) were identified as requiring additional cyber-related skills and knowledge to fully satisfy the requirements of the position. The additional cyber skills are specifically configured to complement the core skills of the designated specialty to characterize fully qualified cyber warriors for each organization's mission.



What Distinguishes Cyber Enlisted Personnel from Others

Specialty (AFS)	Billets	Cyber	Cyber Share
Intel (1N)	148	36	24%
Comm/Computer (2E, 3A, 3C)	203	81	40%
Other	10	1	10%
Grand Total	361	118	33%

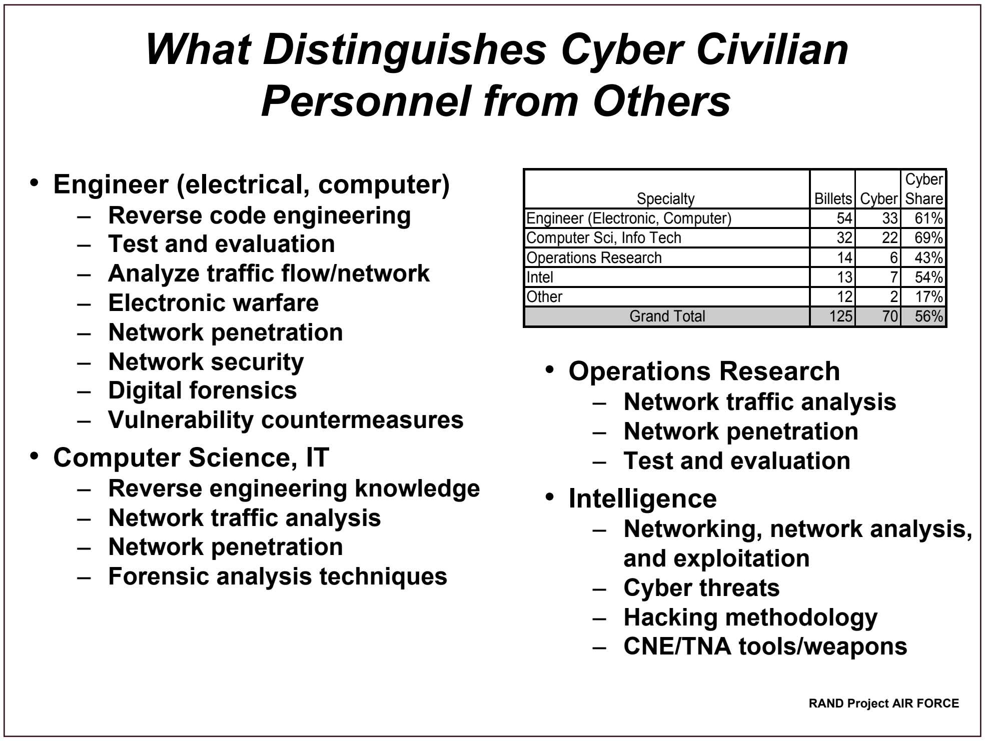
- **Communications-computer**
  - **Network warfare operations**
  - **AOC networks**
  - **TNA and CNA mission planning and execution**
  - **Understand/employ TNA and CNA weapons**
  - **Network mapping and exploitation**
  - **NSA weapons familiarity**
  - **Management of network *attack* system**
- **Intelligence**
  - **Telecommunications infrastructures/network knowledge**
  - **C4 network intelligence**
  - **Network traffic analysis tools**
  - **PSYOP planning processes**
  - **Information operations, including MILDEC**

RAND Project AIR FORCE

DB579-14

Two career fields, communications-computer (AFSCs 2E, 3A, and 3C)[12] and intelligence (AFSC 1N), comprise most of the enlisted billets in the organizations we reviewed. Of the 203 enlisted communications-computer billets reviewed, 81 required cyber-hybrid skills. These positions were distinguished by their additional need for highly specific skills and knowledge of computer networks and ways to exploit and attack networks. The areas of expertise include network warfare operations, AOC networks, computer network attack weapons and mission planning, network mapping and exploitation, familiarity with NSA tool sets, and how to manage network attack systems. Among the 148 intelligence billets reviewed, a smaller proportion (36 of 148) required cyber-hybrid skill sets: telecommunications infrastructures and network knowledge; command, control, communications, and computers (C4) network intelligence; network traffic analysis tools; psychological operations (PSYOP) planning processes; and knowledge about IO. In total, one-third (118 of 361) of the enlisted positions reviewed required additional cyber-related skills.

[12] The communications-computer specialties included communication-electronics (2E), information management (3A), and communication-computer systems (3C).



What Distinguishes Cyber Civilian Personnel from Others

- **Engineer (electrical, computer)**
  - **Reverse code engineering**
  - **Test and evaluation**
  - **Analyze traffic flow/network**
  - **Electronic warfare**
  - **Network penetration**
  - **Network security**
  - **Digital forensics**
  - **Vulnerability countermeasures**
- **Computer Science, IT**
  - **Reverse engineering knowledge**
  - **Network traffic analysis**
  - **Network penetration**
  - **Forensic analysis techniques**

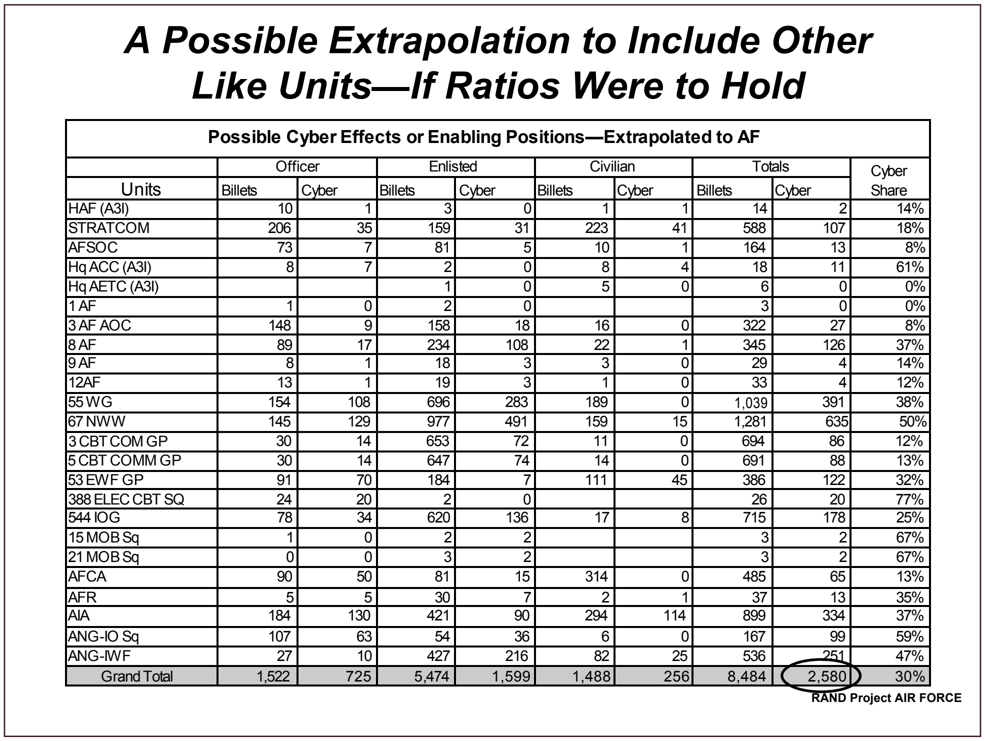
Specialty	Billets	Cyber	Cyber Share
Engineer (Electronic, Computer)	54	33	61%
Computer Sci, Info Tech	32	22	69%
Operations Research	14	6	43%
Intel	13	7	54%
Other	12	2	17%
Grand Total	125	70	56%

- **Operations Research**
  - **Network traffic analysis**
  - **Network penetration**
  - **Test and evaluation**
- **Intelligence**
  - **Networking, network analysis, and exploitation**
  - **Cyber threats**
  - **Hacking methodology**
  - **CNE/TNA tools/weapons**

RAND Project AIR FORCE

DB579-15

We also gathered skill requirements data for a small and highly specialized set of civilian billets. Most of these positions are found in the AFIOC. They are responsible for the creation of cyber-enabling capabilities in the 318th IO Group, and many require cyber-hybrid skills. Of the 125 civilian billets formally requiring engineering, computer science, information technology, operations research, intelligence, or program analyst specialties, 56 percent (70 of 125) were identified as requiring additional cyber skills. Electrical and computer engineer billets required additional skills and knowledge pertaining to networks, reverse code engineering, test and evaluation (T&E), vulnerability countermeasures, and EW. Many of the computer science, IT, and operations research positions also required these skills. Just over half of the civilian intelligence positions required additional skills pertaining to cyber threats and threat methods, as well as knowledge of networks and network exploitation.



A Possible Extrapolation to Include Other Like Units—If Ratios Were to Hold

Possible Cyber Effects or Enabling Positions—Extrapolated to AF

	Officer		Enlisted		Civilian		Totals		Cyber
Units	Billets	Cyber	Billets	Cyber	Billets	Cyber	Billets	Cyber	Share
HAF (A3I)	10	1	3	0	1	1	14	2	14%
STRATCOM	206	35	159	31	223	41	588	107	18%
AFSOC	73	7	81	5	10	1	164	13	8%
Hq ACC (A3I)	8	7	2	0	8	4	18	11	61%
Hq AETC (A3I)			1	0	5	0	6	0	0%
1 AF	1	0	2	0			3	0	0%
3 AF AOC	148	9	158	18	16	0	322	27	8%
8 AF	89	17	234	108	22	1	345	126	37%
9 AF	8	1	18	3	3	0	29	4	14%
12AF	13	1	19	3	1	0	33	4	12%
55 WG	154	108	696	283	189	0	1,039	391	38%
67 NWW	145	129	977	491	159	15	1,281	635	50%
3 CBT COM GP	30	14	653	72	11	0	694	86	12%
5 CBT COMM GP	30	14	647	74	14	0	691	88	13%
53 EWF GP	91	70	184	7	111	45	386	122	32%
388 ELEC CBT SQ	24	20	2	0			26	20	77%
544 IOG	78	34	620	136	17	8	715	178	25%
15 MOB Sq	1	0	2	2			3	2	67%
21 MOB Sq	0	0	3	2			3	2	67%
AFCA	90	50	81	15	314	0	485	65	13%
AFR	5	5	30	7	2	1	37	13	35%
AIA	184	130	421	90	294	114	899	334	37%
ANG-IO Sq	107	63	54	36	6	0	167	99	59%
ANG-IWF	27	10	427	216	82	25	536	251	47%
Grand Total	1,522	725	5,474	1,599	1,488	256	8,484	2,580	30%

RAND Project AIR FORCE

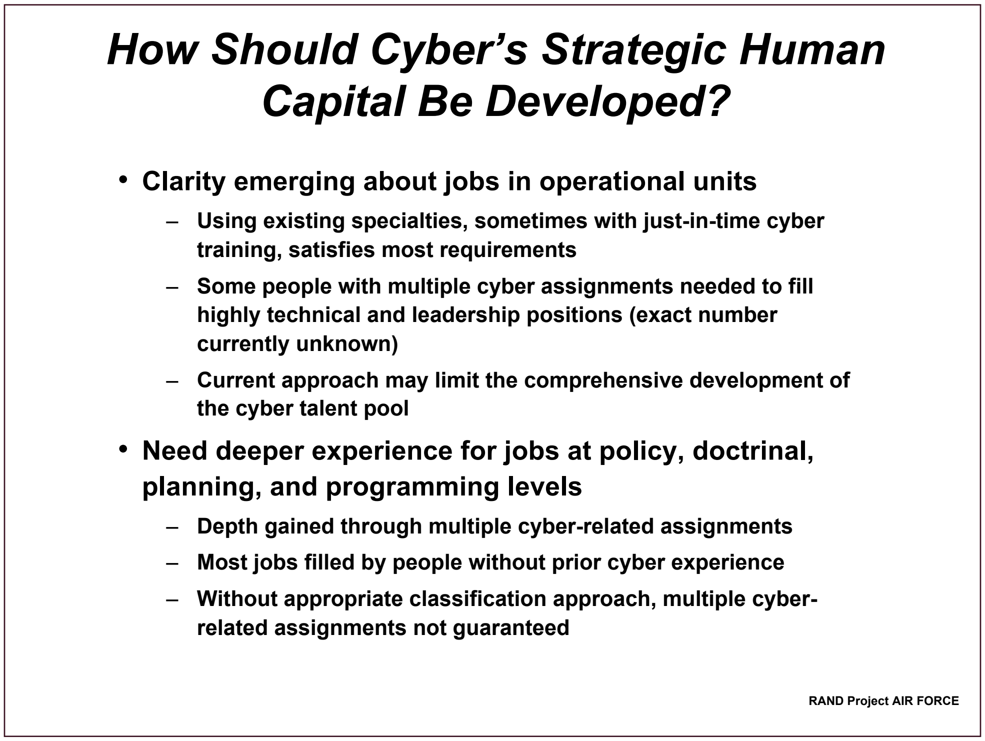
DB579-16

Extrapolating to Similar Organizations

We then estimated the total number of cyber-hybrid positions likely to exist throughout the Air Force. First, we determined the cyber-hybrid-to-core specialty ratios by grade for each organization in the sample.[13] Next, we designated potential cyber organizations that were not in the sample as similar or near-similar to organizations in the sample. Then we applied the appropriate ratios to the core specialties in each organization. The results are shown in this slide.

This approach estimates roughly 2,600 cyber-hybrid jobs, given the then-existing missions, concepts of operations, and organizations. Inevitable changes to the missions, concepts of operations, and organizations will dictate revised estimates. As mentioned earlier, the human capital management of the cyber force will be strongly influenced by the current and desired future size and composition of the cyber force.

[13] For example, the Numbered Air Forces Headquarters were considered similar to the 8th Air Force Headquarters. As another example, the AOCs were considered similar to the 8th Air Force AOC.



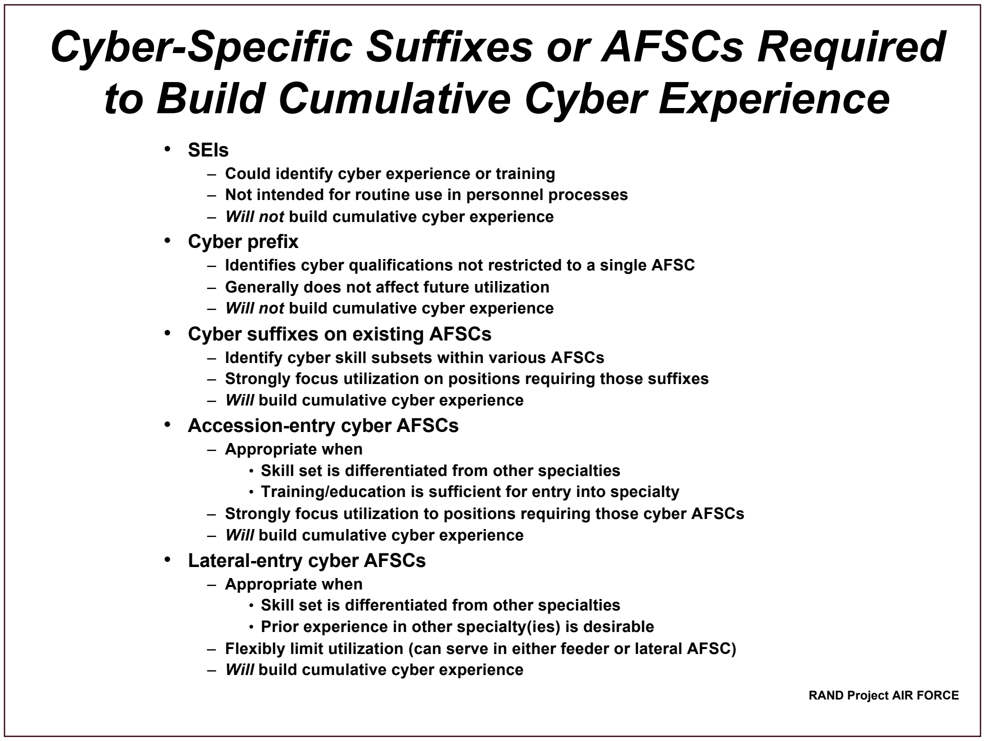
How Should Cyber's Strategic Human Capital Be Developed?

- **Clarity emerging about jobs in operational units**
  - **Using existing specialties, sometimes with just-in-time cyber training, satisfies most requirements**
  - **Some people with multiple cyber assignments needed to fill highly technical and leadership positions (exact number currently unknown)**
  - **Current approach may limit the comprehensive development of the cyber talent pool**
- **Need deeper experience for jobs at policy, doctrinal, planning, and programming levels**
  - **Depth gained through multiple cyber-related assignments**
  - **Most jobs filled by people without prior cyber experience**
  - **Without appropriate classification approach, multiple cyber-related assignments not guaranteed**

RAND Project AIR FORCE

DB579-17

The results of the billet review provided insights about how cyber human capital is currently being developed and where enhancements to development strategies are needed. Currently, development is decentralized and specifically tailored to each organization's needs. The cyber organizations we reviewed have two types of billets: those with requirements largely limited to skills from traditional specialties and those that require an augmentation of traditional specialty skills with skills and knowledge associated with specific cyber capabilities. Typically, this augmentation is provided by the local organizations, which devise their own unit-level training for necessary cyber skills. However, some leadership positions and highly technical billets in these organizations require personnel with in-depth cyber knowledge and skills acquired through multiple assignments. Current classification and assignment procedures provide no systematic way of assuring repeated assignments in cyber-related jobs. While the decentralized approach to development seems to satisfy most local requirements, it cannot adequately address local requirements for greater depth. There is also a lack of in-depth cyber experience at higher levels in the Air Force, particularly for jobs at policy, doctrinal, planning, and programming levels. Such positions also require skills and knowledge gained through multiple cyber-related assignments. However, at the time of this research, most of the positions were filled by people without prior cyber experience. To address these shortfalls, the Air Force may need to adopt an approach to classifying cyber skill requirements and cyber personnel that will support comprehensive development of the cyber force.



Cyber-Specific Suffixes or AFSCs Required to Build Cumulative Cyber Experience

- SEIs
  - Could identify cyber experience or training
  - Not intended for routine use in personnel processes
  - *Will not* build cumulative cyber experience
- Cyber prefix
  - Identifies cyber qualifications not restricted to a single AFSC
  - Generally does not affect future utilization
  - *Will not* build cumulative cyber experience
- Cyber suffixes on existing AFSCs
  - Identify cyber skill subsets within various AFSCs
  - Strongly focus utilization on positions requiring those suffixes
  - *Will* build cumulative cyber experience
- Accession-entry cyber AFSCs
  - Appropriate when
    - Skill set is differentiated from other specialties
    - Training/education is sufficient for entry into specialty
  - Strongly focus utilization to positions requiring those cyber AFSCs
  - *Will* build cumulative cyber experience
- Lateral-entry cyber AFSCs
  - Appropriate when
    - Skill set is differentiated from other specialties
    - Prior experience in other specialty(ies) is desirable
  - Flexibly limit utilization (can serve in either feeder or lateral AFSC)
  - *Will* build cumulative cyber experience

RAND Project AIR FORCE

DB579-18

Building Cumulative Cyber Experience

The Air Force has five specialty-related mechanisms to help manage human capital: special experience identifiers (SEIs), skill prefixes linked to several AFSCs, suffixes linked to specific AFSCs, accession-entry AFSCs, and lateral-entry AFSCs. We evaluated the alternatives against three criteria: (1) capability to identify specific skill sets, (2) appropriateness for workforce management and utilization, and (3) ability to build cumulative experience.

SEIs are used to identify special experience or training not otherwise identified in the personnel data system. They permit rapid identification of individuals already experienced to meet peacetime assignments or identify critical manning requirements during wartime or contingency operations (DAF, 2006, p. 26).[14] Although some SEIs are used to record the development of complex skills, they are not used routinely in personnel processes, nor are they designed as a substitute for an AFSC. Consequently, SEIs do not provide a ready means to track the acquisition of a wide array of skills associated with an occupational or functional area. If used in their current form to manage cyber human capital, they would not result in the building of cumulative cyber experience.

A prefix is a letter designation that is used as part of an AFSC to identify an ability, special qualification, or system. For example, personnel assigned to formal training course instructor

[14] For example, the Air Force currently assigns the network defense capability specialist SEI (9J) to officers in the intelligence, communications-computer, developmental engineering, and special investigator career fields. To qualify for the SEI, officers must either complete a network operator basic school or have been assigned in a network defense capability specialist position for 11 months. Special investigation officers must also complete an information warfare applications course to be awarded the SEI.

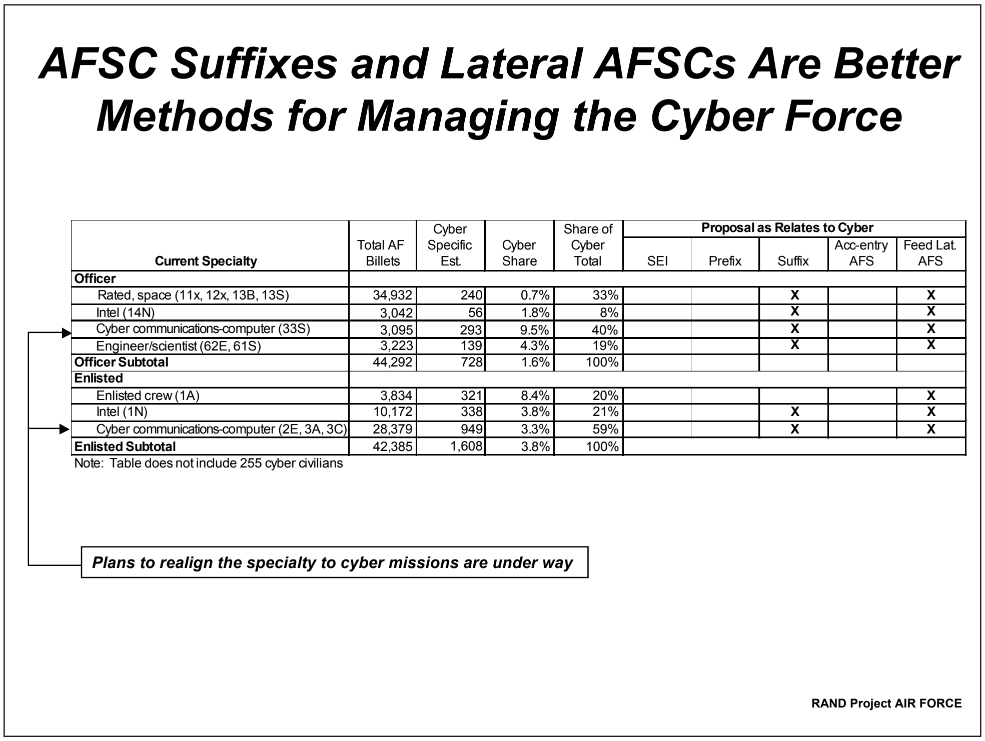
positions are awarded a prefix to their AFSC. The use of prefixes is not restricted to a single AFSC, but the prefixes do not affect future utilization of personnel. Currently the E prefix, electronic combat support duty, and the U prefix, information operations, have the most direct application to identifying cyber skills.[15] If these prefixes or new prefixes are used to manage the cyber force, they could accurately characterize current cyber-hybrid skills held by intelligence or communications-computer personnel. However, since the prefix would not be used to guide their future assignments, its use would not build cumulative cyber experience.

An AFSC suffix is also an alphabetical code that is used as part of the AFSC to specify skill subsets (e.g., equipment or functions and positions) within an AFSC. Each suffix has a title and its use for human capital management is to ensure focused utilization of personnel in positions requiring that suffix. Many AFSCs require the use of a suffix, but in some cases the suffix is optional. An example of this in the officer classification system is AFSC 21M, Munitions and Missile Maintenance. It may be used without a suffix, or the C suffix may be added to indicate nuclear-related skills. Similarly, a cyber suffix used in conjunction with AFSCs commonly associated with the cyber mission could be used to build cumulative cyber experience within those AFSCs.

An accession-entry AFSC is awarded upon completion of requisite training or certification, usually soon after induction into the Air Force. This method of human capital management is appropriate when enough positions require common qualifications and skills that are distinct from other specialties and where training or education is sufficient for entry into the specialty. As a method of human capital management, accession-entry-level AFSCs are used to ensure proper assignment of personnel to positions requiring that AFSC. Consequently, the creation of an accession-entry cyber AFSC would build cumulative cyber experience for the Air Force.

A lateral AFSC is typically awarded to personnel who have qualified previously in another AFSC. Its use in managing the cyber force would be to systematically identify specific cyber-hybrid skills among experienced personnel in related specialties. Because its purpose would be to broaden and enhance the utilization of personnel, a lateral AFSC would contribute to building cumulative cyber experience. AFSC 16R, Planning and Programming, is an example of an officer lateral AFSC that accepts entry from any other AFSC. AFSC 3S1X1, Military Equal Opportunity, is an example of a similar enlisted AFSC.

[15] The prefix E identifies positions in manning documents and officers serving in, or qualified to serve in, positions requiring the ability to plan, collect, analyze, and apply intelligence support to electronic combat operations or the research, development, and acquisition of U.S. electronic combat forces. The prefix U identifies positions on manpower documents and officers serving in, or qualified to serve in, positions requiring IO expertise and knowledge to gain, exploit, defend, and attack information and information systems (DAF, 2004, pp. 32, 43).



AFSC Suffixes and Lateral AFSCs Are Better Methods for Managing the Cyber Force

Current Specialty	Total AF Billets	Cyber Specific Est.	Cyber Share	Share of Cyber Total	Proposal as Relates to Cyber				
					SEI	Prefix	Suffix	Acc-entry AFS	Feed Lat. AFS
Officer									
Rated, space (11x, 12x, 13B, 13S)	34,932	240	0.7%	33%			X		X
Intel (14N)	3,042	56	1.8%	8%			X		X
Cyber communications-computer (33S)	3,095	293	9.5%	40%			X		X
Engineer/scientist (62E, 61S)	3,223	139	4.3%	19%			X		X
Officer Subtotal	44,292	728	1.6%	100%					
Enlisted									
Enlisted crew (1A)	3,834	321	8.4%	20%					X
Intel (1N)	10,172	338	3.8%	21%			X		X
Cyber communications-computer (2E, 3A, 3C)	28,379	949	3.3%	59%			X		X
Enlisted Subtotal	42,385	1,608	3.8%	100%					

Note: Table does not include 255 cyber civilians

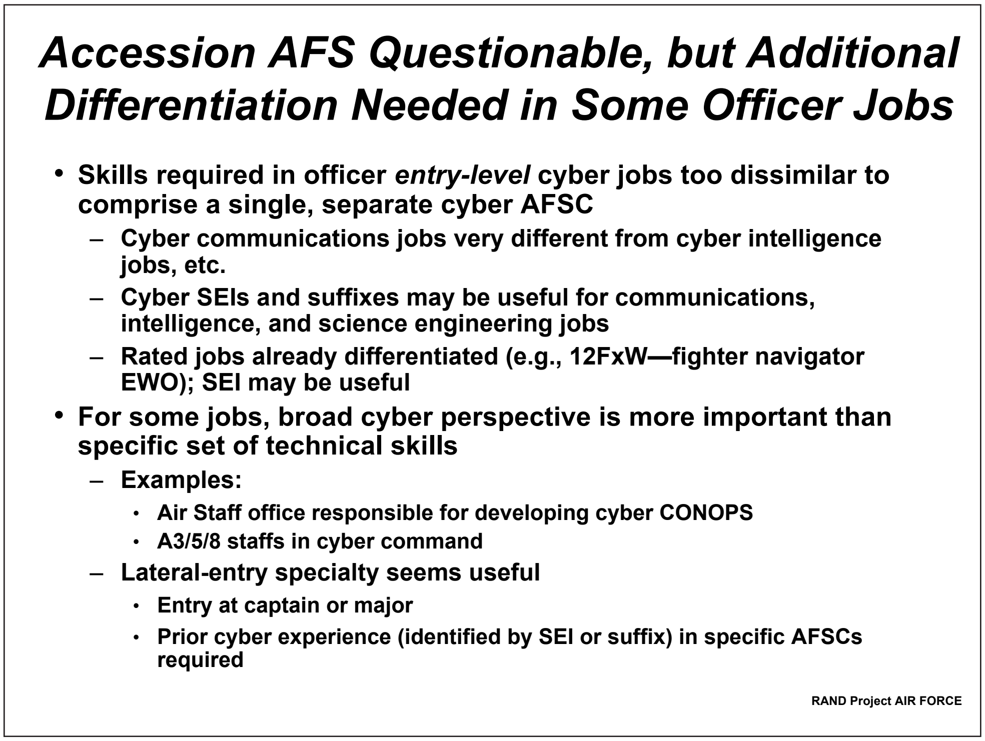
Plans to realign the specialty to cyber missions are under way

RAND Project AIR FORCE

DB579-19

Our analysis of these skill management methods led to the conclusion that AFSC suffixes and the establishment of lateral AFSCs would generally be the preferred methods for managing the cyber force, at least over the next several years.

Each Air Force specialty that is associated with cyber missions is already managed through some combination of SEIs, prefixes, suffixes, and AFSC award processes. The question that should be answered for managing the cyber force is which of these methods would work best in concert with current specialty-specific methods of skills management and development while also contributing to the goals of building a robust, sustainable cyber force. We concluded that SEIs and prefixes are unsuitable because they typically do not contribute to building a future force. Expanding existing accession-entry AFSCs to include cyber-specific skills is also impractical unless the specialty is realigned to be fully integrated with cyber missions. Plans for such realignment are under way for the communications-computer career field but not for other career fields related to cyber missions. We determined that suffixes can be used effectively for the intelligence, communications-computer, and developmental engineering specialties, while lateral AFSCs can contribute to cyber force development goals for all associated specialties. In the pages that follow, we provide our rationale for these conclusions.



Accession AFS Questionable, but Additional Differentiation Needed in Some Officer Jobs

- **Skills required in officer *entry-level* cyber jobs too dissimilar to comprise a single, separate cyber AFSC**
  - **Cyber communications jobs very different from cyber intelligence jobs, etc.**
  - **Cyber SEIs and suffixes may be useful for communications, intelligence, and science engineering jobs**
  - **Rated jobs already differentiated (e.g., 12FxW—fighter navigator EWO); SEI may be useful**
- **For some jobs, broad cyber perspective is more important than specific set of technical skills**
  - **Examples:**
    - **Air Staff office responsible for developing cyber CONOPS**
    - **A3/5/8 staffs in cyber command**
  - **Lateral-entry specialty seems useful**
    - **Entry at captain or major**
    - **Prior cyber experience (identified by SEI or suffix) in specific AFSCs required**

RAND Project AIR FORCE

DB579-20

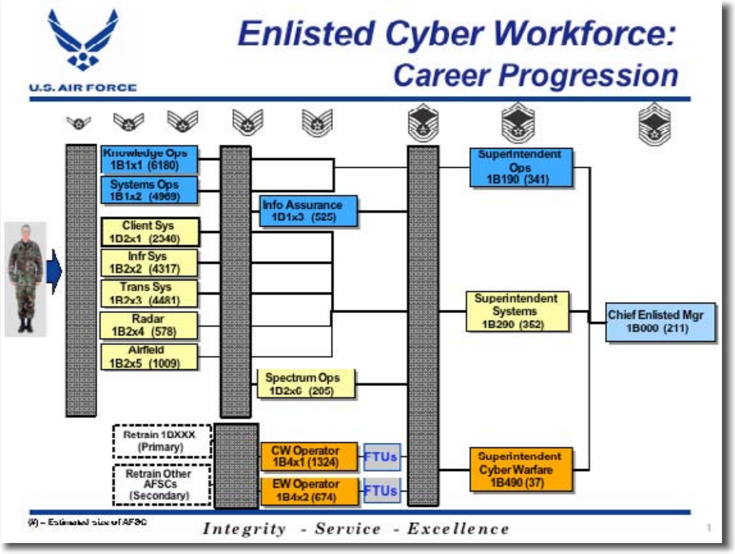
During the course of this research, the Air Force was establishing an accession-entry cyber specialty. We question this approach for managing cyber officers, although we recognize the need for additional differentiation in some officer jobs. The principal argument against an accession-entry AFSC comes from our analysis of cyber position skill requirements. Officer entry-level cyber jobs generally require significant proportions of the skills encompassed within the specific communications-computer, intelligence, or engineer/scientist AFSCs that currently identify the jobs. Collectively, these skills are too disparate and too numerous to form a single, separate cyber AFSC. Instead, cyber suffixes within these AFSCs or (as a last resort) SEIs would be most useful for differentiating the cyber skills required for these positions.

Rated jobs associated with cyber missions are also very dissimilar to other cyber officer positions. For example, knowledge of airmanship, flight operations, and how to execute missions associated with these jobs sets them apart from network operations and network warfare jobs that require knowledge of cyber threats, hacking methodologies, and computer network exploitation tools. However, rated specialties are already managed with a highly differentiated AFSC suffix system, and the appropriate rated suffix seems to be useful in specifying the rated background that is useful in various cyber-related positions. Consequently, if needed, the use of cyber SEIs would provide the additional level of skill differentiation needed to manage rated personnel with cyber skills.

Attention also needs to be directed to officer jobs that require broad cyber perspectives rather than specific sets of technical skills. Example of such jobs include Air Staff offices responsible for developing cyber CONOPS and the A3/5/8 staffs in a cyberspace organization.

Human capital for these jobs should be developed and managed through creation of a lateral cyber specialty. Officers at the senior captain or major level would be selected for entry into a lateral cyber specialty based upon prior cyber experience identified through an SEI or an AFSC suffix.

Enlisted Lateral-Entry Cyber Specialty Included in Revamped Cyber-Communications-Computer AFSC Structure



U.S. AIR FORCE

Enlisted Cyber Workforce: Career Progression

Knowledge Ops 1B1x1 (6180)

Systems Ops 1B1x2 (4969)

Client Sys 1D2x1 (2340)

Infr Sys 1B2x2 (4317)

Trans Sys 1B2x3 (4481)

Radar 1B2x4 (578)

Airfield 1B2x5 (1009)

Info Assurance 1D1x3 (525)

Spectrum Ops 1D2x0 (205)

Retrain 1DXXX (Primary)

Retrain Other AFSCs (Secondary)

CW Operator 1B4x1 (1324)

EW Operator 1B4x2 (674)

FTUs

FTUs

Superintendent Ops 1B190 (341)

Superintendent Systems 1B290 (352)

Superintendent Cyber Warfare 1B490 (37)

Chief Enlisted Mgr 1B000 (211)

(#) – Estimated size of AFSC

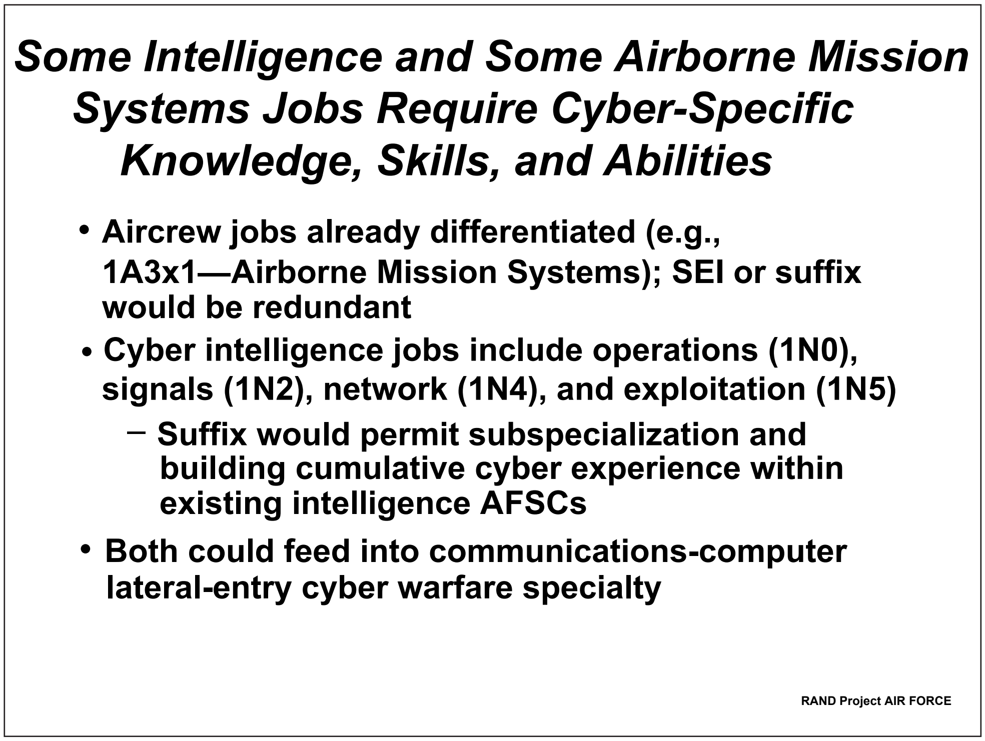
Integrity - Service - Excellence

1

RAND Project AIR FORCE

DB579-21

The enlisted cyber force may be more amenable to accession-entry AFSCs and lateral-entry AFSC management methods, particularly the communications-computer specialty. The diagram in this slide is taken from an Air Force briefing that describes how the communications-computer career field will be restructured for consistency with expected cyber skill requirements. In the plan, personnel coming into the new career field will first receive IT and cyber fundamental training, followed by initial skills training for a specific cyber-communications-computer AFSC award. The plan also incorporates lateral AFSC management of cyber operations skills by allowing some holders of the seven cyber communications-computer AFSCs to transfer to the newly created cyber warfare operator and electronic warfare operator AFSCs at the staff sergeant level. Personnel from other specialties, such as intelligence or enlisted aircrew, could also laterally transfer into the new cyber specialties.



Some Intelligence and Some Airborne Mission Systems Jobs Require Cyber-Specific Knowledge, Skills, and Abilities

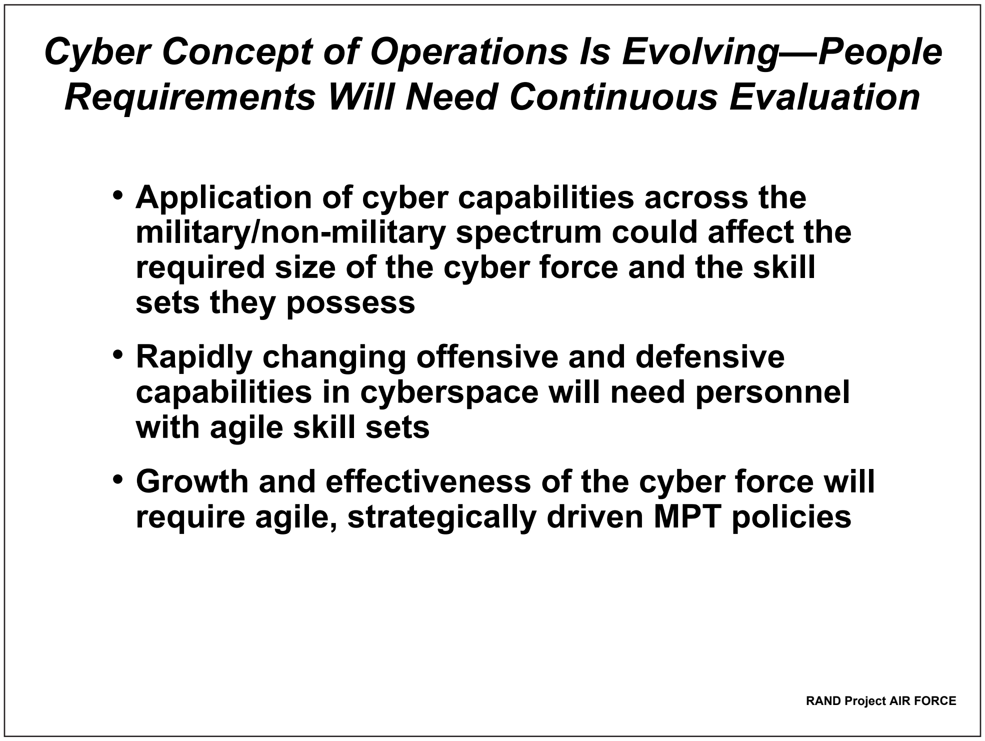
- **Aircrew jobs already differentiated (e.g., 1A3x1—Airborne Mission Systems); SEI or suffix would be redundant**
- **Cyber intelligence jobs include operations (1N0), signals (1N2), network (1N4), and exploitation (1N5)**
  - **Suffix would permit subspecialization and building cumulative cyber experience within existing intelligence AFSCs**
- **Both could feed into communications-computer lateral-entry cyber warfare specialty**

RAND Project AIR FORCE

DB579-22

The enlisted aircrew and intelligence candidates for lateral entry would come from a pool of personnel who have already performed in jobs that require cyber-specific knowledge and skills. Skill management for aircrew jobs is sufficiently differentiated, and the use of an additional SEI or suffix to manage the cyber-related skills (e.g., airborne mission systems) within the specialty would be redundant. However, management of cyber-related skills for intelligence jobs could benefit from additional differentiation. Jobs designated as operations (AFSC 1N0), signals (AFSC 1N2), network (AFSC 1N4), and exploitation (AFSC 1N5) could use a cyber suffix to permit subspecialization and build cumulative cyber experience within the intelligence career field.[16] The current method of differentiating skills for aircrew jobs and the introduction of cyber suffixes for intelligence jobs would allow more-accurate identification of personnel to feed into the lateral-entry cyber warfare specialty.

[16] Initially, we recommend one common suffix among these specialties. As the concept matures, greater differentiation may become necessary. The ultimate number of suffixes should be guided by the concepts of functional grouping and practical specialization.



Cyber Concept of Operations Is Evolving—People Requirements Will Need Continuous Evaluation

- **Application of cyber capabilities across the military/non-military spectrum could affect the required size of the cyber force and the skill sets they possess**
- **Rapidly changing offensive and defensive capabilities in cyberspace will need personnel with agile skill sets**
- **Growth and effectiveness of the cyber force will require agile, strategically driven MPT policies**

RAND Project AIR FORCE

DB579-23

Future Scenario and Integration Seams

Future Scenario

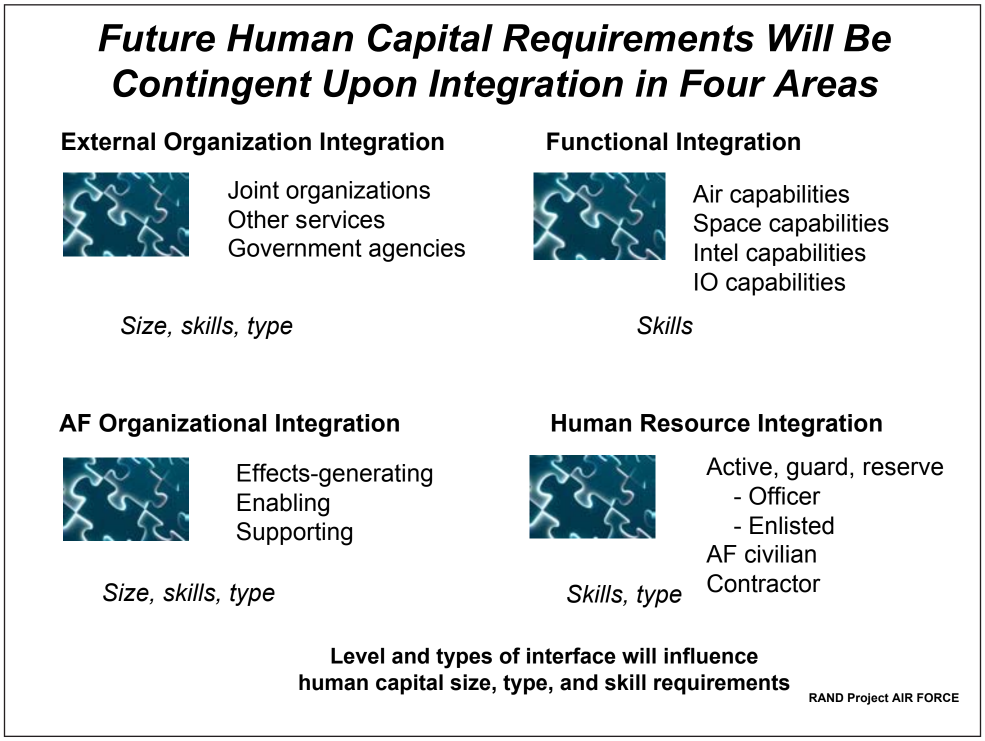
These different skill management methods need to be applied in light of the rapid evolution of cyber concepts of operations. Such evolution suggests that the skills that cyber personnel will require will need continuous evaluation. In an attempt to characterize how cyber skill requirements might evolve, we constructed a cyber capabilities scenario for the year 2020.[17] We propose that cyber capabilities will be fully integrated with conventional kinetic operations. Cyber CONOPS and tactics, techniques, and procedures (TTP) will have been refined from an effects-based perspective to be on a par with kinetic means. Cyber operations will also have accompanying means to predict and measure intended effects. They will be part of wide-ranging missions against traditional nation-state and irregular adversaries, such as violent extremists and criminals who pose threats to national security and sovereignty. These threats imply that Air Force cyber capabilities may be employed across the spectrum of military and nonmilitary threats—ranging from direct support of multiple combatant commanders, to indirect support of multiple government agencies, to indirect support of private-sector network service providers. The application of these capabilities could affect the size of the cyber force and the skills personnel possess.

[17] The scenario was developed from (1) the project team members' subject-matter knowledge of IO, information operations, and recent experience observing IW operations, (2) information gathered from subject-matter experts in network operations and cyber security, and (3) characterizations of cyber threats and vulnerabilities published in unclassified documents.

By 2020, cyber operations are expected to cycle rapidly between employing offensive and defensive capabilities. Experts in network security and network operations suggest that the potential sources of attacks will be numerous, the attacks can occur in various forms, and they will occur at different levels of volume and speed. The response to such attacks, however, must be immediate: It must either follow defensive protocols or produce counterattack actions or steps for using the attacks as an opportunity to gather intelligence. In preparation to deliver forces that can perform this range of options, the Air Force will have developed cyber warriors with complex skill sets that meet the NSA's standards for conducting a complete portfolio of network operations. Cyber warriors will also possess complementary knowledge in air and space operations, IW, PSYOP, strategic communication, and the interdependence and synergy among network attack, defense, and exploitation. They will also have the ability to shift seam¬lessly from being a sensor to a shooter in cyberspace and be grounded in the legal and approvals process associated with Title 10 and Title 50 responsibilities and authorities.[18]

We believe that the growth of a cyber force that can reliably produce capabilities envisioned in this scenario will require the formation and implementation of agile, strategically driven manpower, personnel, and training policies over the next four to six years. In particular, more work will be required in classification policy. As cyber capabili¬ties mature, and the cyber career field develops, the Air Force will need to create more-explicit definitions of cyber specialties.

[18] Title 10, United States Code, Armed Forces, addresses the command authority, jurisdictions, missions, and discipline authority for the military. U.S. Code Title 50, War and National Defense, Chapter 36, addresses electronic surveillance authorization during peacetime and war.



Future Human Capital Requirements Will Be Contingent Upon Integration in Four Areas

External Organization Integration

Joint organizations
Other services
Government agencies

Size, skills, type

Functional Integration

Air capabilities
Space capabilities
Intel capabilities
IO capabilities

Skills

AF Organizational Integration

Effects-generating
Enabling
Supporting

Size, skills, type

Human Resource Integration

Active, guard, reserve
- Officer
- Enlisted

AF civilian
Contractor

Skills, type

Level and types of interface will influence human capital size, type, and skill requirements

RAND Project AIR FORCE

DB579-24

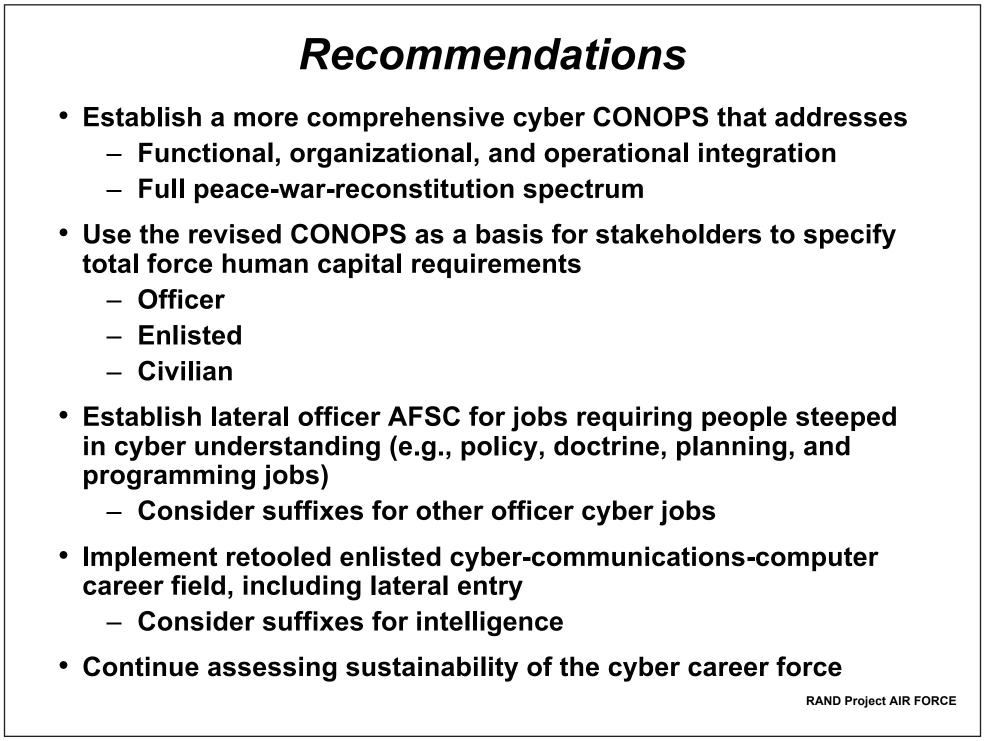
Integration Seams

At a strategic level, accurately defining future cyber human capital requirements will be contingent upon the Air Force's successful integration in four areas. First, it must integrate its capabilities and CONOPS with those of external organizations such as Joint organizations, other services, and other government agencies. Issues range from developing cyber doctrine and CONOPS that are consistent with Joint doctrine, through avoiding unnecessary duplication of capabilities, to establishing how the Air Force will interface with other services and agencies. We expect that resolution of these integration efforts will influence the required size of the cyber force, the specific cyber skills they need to possess, and the types of personnel that comprise the core of the force (i.e., officer, enlisted, civilian, reserve, guard).

Next, in order for cyber operations to be integrated with kinetic operations, the Air Force must examine functional integration requirements. Cyber capabilities need to be integrated with air, space, intelligence, and IO capabilities to fully realize the Air Force's vision of an air, space, and cyberspace force. This integration audit should more precisely identify the skills, particularly cyber-hybrid skills, required to produce cyber capabilities.

Future human capital requirements will also be shaped by how cyber-related organizations across the Air Force are integrated to produce nonkinetic effects. Specifying how effects-generating cyber organizations (e.g., 67th NWW) will operate in conjunction with cyber-enabling organizations (e.g., AFIOC) and cyber-supporting organizations (e.g., the Global CyberSpace Integration Center) should improve the development of requirements-based nonkinetic capabilities. This specification is also likely to influence the size, skill composition, and type requirements for the cyber human capital that will generate and support these capabilities.

Finally, the Air Force should develop a clear strategy for integrating the different types of human capital that make up the cyber force. Currently, personnel from each service category and contractors engage in most aspects of developing cyber capabilities and performing cyber missions. However, future cyber capabilities may guide the mix of human capital from reserve components, Air Force civilians, and contractors in ways that maximize the skill sets these personnel possess and, ultimately, the configuration of the types of human capital that make up the cyber force. Reserve component members who are employed in industries related to cyber operations can be tapped to provide the most current knowledge, tools, and techniques for network warfare operations. Air Force civilians and contractors can offer depth and breadth of organizational experience to sustain the development and application of cyber tools and techniques.



Recommendations

- Establish a more comprehensive cyber CONOPS that addresses
  - Functional, organizational, and operational integration
  - Full peace-war-reconstitution spectrum
- Use the revised CONOPS as a basis for stakeholders to specify total force human capital requirements
  - Officer
  - Enlisted
  - Civilian
- Establish lateral officer AFSC for jobs requiring people steeped in cyber understanding (e.g., policy, doctrine, planning, and programming jobs)
  - Consider suffixes for other officer cyber jobs
- Implement retooled enlisted cyber-communications-computer career field, including lateral entry
  - Consider suffixes for intelligence
- Continue assessing sustainability of the cyber career force

RAND Project AIR FORCE

DB579-25

Recommendations

In total, our findings support the following recommendations. The cyber CONOPS does not sufficiently address the complexities of cyber vulnerabilities, cyber threats, or cyber warfare. Although we acknowledge that these concepts are evolving with many unknowns, the Air Force should establish a more comprehensive CONOPS that addresses the functional, organizational, and operational integration needed to create capabilities. Articulating this kind of integration should surface inherent strengths that the Air Force should enhance and opportunities to develop capabilities in EW, computer network defense, and computer network exploitation.

The Air Force should also plan for broad application of its cyber capabilities. It is reasonable to expect that many cyber capabilities created and delivered by the Air Force will be employed before any hostile actions are authorized, particularly in the area of computer network defense. But other peacetime capabilities are also important, such as support to law enforcement, cyber-based research, development, test, and evaluation (RDT&E), and cyber forensics capabilities. During periods of hostility, we expect cyber capabilities to be used in myriad forms, but there is likely to be a continued need for cyber capabilities during reconstitution from hostilities, particularly in cases of IW and counterinsurgency. Consequently, the CONOPS should also address how the Air Force will operate in and through cyberspace throughout the peace-war-reconstitution spectrum of activities. The revised CONOPS can then be used as a basis for stakeholders to specify the appropriate total force mix (i.e., active duty, reserve components, Air Force civilians, contractors) in the cyber force.

Next, we recommend that the Air Force 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 understanding. Officers awarded this AFSC will form the pool of leadership who, throughout the rest of their careers, will gain knowledge and experience in cyber operations from an interservice and interagency perspective and will then leverage those skills to enhance the development of the Air Force's cyber capabilities. We also recommend that the Air Force use AFSC suffixes to manage cyber skills for other officer jobs.

The results of our study also support the implementation of the retooled enlisted communications-computer career field. The realignment of occupational specialties within the career field to cyber capabilities and the plan for a lateral-entry AFSC for EW operations and network operations are sound. However, use of an AFSC suffix should be sufficient for managing cyber skills within the intelligence career field.

Overall, the Air Force has much to do to create a sustainable, skilled cyber force that can create the capabilities suggested by its vision. Whether it manages that force through the creation of a new AF cyber specialty or effectively manages the cyber skill sets of airmen within current specialties, it must be vigilant in its efforts to create cyber warriors, particularly within the next four to six years.

Our final recommendation is for continued assessment of the sustainability of the cyber force. At the time of this research, the cyberspace human capital force structure had not yet been completed. Targets for types of manpower, specialties, training, and grade-skill mixes had not been fully specified. Furthermore, a thorough identification of the actual cyber workforce was still under way. When these activities are completed, the Air Force can begin to identify whether the supply of cyber human capital falls short of its desired targets. Then it can develop accession, utilization, and retention policies to maintain the viability of its cyber force.

References

8th Air Force, "Air Force Cyber Operations Command," briefing, December 13, 2006.

Bush, George W., *The National Strategy to Secure Cyberspace,* Washington, D.C., 2003.

DAF—*see* Department of the Air Force.

Department of the Air Force (DAF), *Officer Classification,* Washington, D.C.: Air Force Manual (AFM) 36-2105, 2004.

———, *Information Operations,* Washington, D.C.: Air Force Doctrine Document (AFDD) 2-5, January 11, 2005.

———, *Classifying Military Personnel (Officer and Enlisted),* Washington, D.C.: Air Force Instruction (AFI) 36-2101, 2006.

JCS—*see* Joint Chiefs of Staff.

Joint Chiefs of Staff (JCS), *The National Military Strategy of the United States of America,* Washington, D.C., 2004.

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms,* Washington, D.C., 2008.

Joint Publication 3-13, *Information Operations,* Washington, D.C., 2006.

Joint Publication 3-13.1, *Electronic Warfare,* Washington, D.C., 2007.

JP—*see* Joint Publication.

Robbert, Albert A., Steve Drezner, John E. Boon, Jr., Lawrence M. Hanser, S. Craig Moore, Lynn M. Scott, and Herbert J. Shukiar, *Integrated Planning for the Air Force Senior Leader Workforce: Background and Methods,* Santa Monica, Calif.: RAND Corporation, TR-175-AF, 2004. As of May 29, 2009: http://www.rand.org/pubs/technical_reports/TR175/

United States Code, Title 10, Armed Forces, 2006.

United States Code, Title 50, Chapter 36, Foreign Intelligence Surveillance, 2006.

U.S. Air Force, *Air Force Cyber Concept of Operations*, Version 4.0, December 21, 2006.